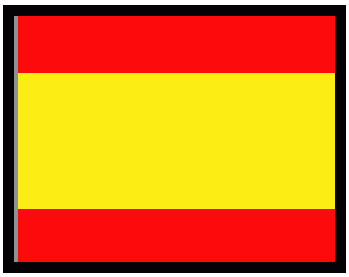

ESPAÑA (SPAIN) : Trusted List

Tsl Id: TSL20211026

Valid until nextUpdate value: 2022-04-25T00:00:00Z

TSL signed on: 2021-10-26T09:34:56Z

PDF generated on: Tue Oct 26 11:38:33 CEST 2021

TSL Scheme Information

TSL Id	*TSL20211026*
TSLTag	*http://uri.etsi.org/19612/TSLTag*
TSL Version Identifier	*5*
TSL Sequence Number	*116*
TSL Type	*http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric*

Scheme Operator Name

Name	*[es]*	*MINISTERIO DE ECONOMIA Y EMPRESA*
Name	*[en]*	*MINISTRY OF ECONOMY AND BUSINESS*

PostalAddress

Street Address	*[en]*	*Poeta Joan Maragall, 41*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28020*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Poeta Joan Maragall, 41*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28020*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.mineco.gob.es*
URI	*[en]*	*mailto:sgssi@mineco.es*

Scheme Name

Name	*[en]*	*ES:Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*
Name	*[es]*	*ES:Lista de confianza que incluye información relacionada con los proveedores de servicios de confianza cualificados que supervisa el Estado miembro de expedición, junto con información relacionada con los servicios de confianza cualificados que estos prestan, de conformidad con las disposiciones pertinentes establecidas en el Reglamento No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.*

Scheme Information URI

URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeinformationURI_es.aspx*
URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeinformationURI_en.aspx*

Status Determination Approach *http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate*

Scheme Type Community Rules

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon*
URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/schemerules/ES*

Scheme Territory *ES*

Policy Or Legal Notice

TSL Legal Notice	*[en]*	*The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*
TSL Legal Notice	*[es]*	*El marco jurídico aplicable a la presente lista de confianza es el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.*

Historical Information Period *65535*

Pointer to other TSL - EUROPEAN UNION

1.EU TSL - MimeType: application/vnd.etsi.tsl+xml

TSL Location *https://ec.europa.eu/tools/lotl/eu-lotl.xml*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *640374569763301965251188002573981856 71*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIBTCCBu2gAwIBAgIQMC0qZHRS96hQhJJbKgWexzANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2l0YWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTcW1hbnR1YyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEtl
IEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEzMCQGA1UEAxMdRGlmaXRhbFNpZ24gUXVhbGlmaWVk
IENBIC0gRzMwHhcNMTkxMjA2MDAwMDAwWhcNMjIxMjA1MjM1OTU5WjCCAZ0xCzAJBgNVBAYTAkdS
MRwwGgYDVQQKFBNFVVJPUEVBTiBDT01NSVNTSU9OMRkwFwYDVQRhFBBWQVRCRS0wOTQ5MzgzMzQy
MT0wOwYDVQQLEzRDZXJ0aWZpY2F0ZSBQcm9maWxlIC0gUXVhbGlmaWVkIENlcnRpZmlj YXRlIC0g
TWVtYmVyMUUwQwYDVQQLEzxUZXJtcyBvZiBlc2UgYXQgaHR0cHM6L y9zd3cuZGlnaXRhbHNpZ24u
cHQvRUNESUdJVEFMU0lHIT09ycGExTAjBgNVBAsUHEVudGlibGVzZW50IC0gREIHSVQgT0ZGSUNJ
QUwxLTArBgkqhkiG9w0BCQEWHmFwb3N0b2xvcyShcGxhZGFzQGVjLmV1cm9wYS5ldTEYMBYGA1UE
BRMPUEFTR1IlQVAzMTQxMDQyMRAwDgYDVQQEFAdBUExBREFTMRIwEAYDVQQqFAIBUE9TVE9MT1Mx
HTAhBgNVBAsUFFJlbW90ZVFTQ0RNYW5hZ2VvZW50MRowGAYDVQQDFBFBUE9TVE9MT1MgQVRMQURB
UzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAO6xZV66wrUkPbn6VLZJcXBtzmMQ8JWt
efuA1Odmd/6MoFY+iiXLwlNZpLr/EQ4Hbcx3i2H0P4RCSfKDtPn3SuCn+tkZPNmavpJ+UMkQ38RK
MErQ9uQGHeHqCsvmQsE+2OplIT2aLaGEA29FkFGaugrq1EEY47KMYhcBn68lUG5teE/eGg7sYh
wV4pFlLf9TULLLcmugVSlFyZmVrAMKcqp5GMj5VXzRjNwYJlNTApSki44VBxvLlkoBcuncIsSj7
CZxNWiHIsUNAGd8U+hcGSr78dlq9rjEj9Wxq6jbc0XakHHmWT2lngPadDIEgstBKJKGofjMqtJ
ZpS2DlsCAwEAAaOCAx4wggMaMAkGA1UdEwQCMAAwcwYDVR0fBGwwajBooGagZIziaHR0cDovL29u
c2l0ZWNybC50cnVzdHdpc2UuY29tL0RpZ2l0YWxTaWduQ2VydGlmaWNhZG9yYURpZ2l0YWxRdWFs
aWZpZWRDZXJ0aWZpY2F0ZUcrL0xhdGVzdFNSTC5jcmwwDgYDVR0PAQH/BAQDAgZAMG4GA1UdIARn
MGUwSQYLYIZIAYb4RQEHFwIwOjA8BggrBgEFBQcCARYsaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24u
cHQvRUNESUdJVEFMU0lHIT09jcHMwDQYLYIZIAYb4RQEHLAIwCQYHBACL7EABAjAdBgNVHQ4EFgQU
9XRl9OH2TD8L lbkA9yWDZwVh01gwHwYDVR0jBBgwFoAU+16OQpwjqH30G4xcIDsYq9nZ90AwKQYD
VR0RBCTwIEeYXBvc3Rvb G9zLmFwbGFkYXNAZWMuZXVvb3BhLmV1MIHmBggrBgEFBQcBAwSB2TCB
1jAVBggrBgEFBQcLAjAJBgcEAIvsSQEBMB1GCCsGAQUFBwsCMAkGBwQAi+xJAQIwCAYGBACORgEB
MAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGATB9BgYEAI5GAQUwczA2FjBodHRwczovL3d3
dy5kaWdpdGFsc2lnbi5wdC9FQ0RJR0lUQUxTSUdOL2Nwcy9kZHATAIBUMDkWM2h0dHBzOi8vd3d3
LmRpZ2l0YWxzaWduLnB0L0VDREIHSVRBTFNJR04vY3BzL2RkcF9lbhMCRU4wHQYDVR0lBBYwFAY1
KwYBBQUHAwIGCCsGAQUFBwMEMGkBggrBgEFBQcBAQSBbzCBlDAJBggrBgEFBQcwAYYdaHR0cDov
L3N0ZC1vYJNwLnRydXNlbd2lzZS5jb20uZwYJKwYBBQUHMAKGW2hbdHAdLy9vbnNpdGVjcmwudHJl
c3R3aXNlLmNvbS9EaWdpdGFsU2lnbkNlcnRpZmlyWRvcmFEaWdpdGFsUXVhbGlmaWVkQ2VydGlm
aWNhdGVHMy9jYS5jcnQwDQYJKoZIhvcNAQELBQADggEBAFRKyVFYQIs8kXxsuyQ47BcoyKJ0JZEP
qcgJWyUg3pJSeKdS0q3fcP9nlI4Nlt3wFrYQdK6dO12nFg6cuuY+SVDafhpGtJV5TEctvRK84Bk
Wab2RdarGh3MIdcSV0sbxan8rmknWf87qUkDt+1OrqLAJqTKT6/g/O7GASxFMQMp88Vw6KoV6P9z
IbcvejYI7IE/JdEmKA30zwaAc6pJ270v6YLFnDKrr9Rgfs6RZ6mG27XSMKOvb2Ax4+eUGCv57FFA
A3FGLphsTQ9mkD4zZwaSTmaUzvY2M5K65JIjLpKbzdUulHbQGDbX79GTsmDKsAYdKZe+UacNFl
/5Tx7ko=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G3*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *APOSTOLOS APLADAS*

Subject OU: *RemoteQSCDManagement*

Subject GIVEN NAME: *APOSTOLOS*

Subject SURNAME: *APLADAS*

Subject SERIAL NUMBER: *PASGR-AP3141042*

Subject E: *apostolos.apladas@ec.europa.eu*

Subject OU: *Entitlement - DIGIT OFFICIAL*

Subject OU: *Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa*

Subject OU: *Certificate Profile - Qualified Certificate - Member*

Subject 2.5.4.97: *VATBE-0949383342*

Subject O: *EUROPEAN COMMISSION*

Subject C:	*GR*
Valid from:	*Fri Dec 06 01:00:00 CET 2019*
Valid to:	*Tue Dec 06 00:59:59 CET 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EE:B1:65:5E:9F:C3:05:24:3F:49:FA:54:B6:49:CD:70:5B:CE:73:10:F0:95:AD:79:FB:80:20:E7:66:74:9E:8C:A0:56:3E:8A:25:CB:C2:53:59:A4:BA:FF:11:0E:07:85:CC:77:8B:61:F4:3F:84:42:49:F2:83:B4:F9:F7:4A:E0:A7:FA:D9:19:3C:D9:9A:BE:92:7E:50:C9:10:DF:C4:4A:30:4A:D0:F6:E4:06:1D:E1:EA:0A:CB:EB:9D:0B:04:FB:63:A9:22:54:F6:68:B6:86:7F:F0:36:F4:59:05:1A:EB:A0:AE:AD:44:11:8E:3B:28:C6:21:70:19:FA:F2:55:06:E6:D7:84:FD:E1:A0:EE:C6:21:C1:5E:29:16:52:DF:7F:D4:D4:2C:B2:DC:9A:E8:15:4A:51:63:66:65:6B:00:C2:9C:AA:9E:46:32:3E:55:5F:34:63:37:06:09:20:D4:C0:A5:29:22:E3:85:41:C6:F2:E5:92:80:5C:BA:77:08:B1:28:FB:09:9C:4D:5A:21:C8:B1:43:40:19:DF:14:FA:5C:46:4A:BE:C1:76:5A:BD:AE:31:23:F5:6C:6A:EA:36:DC:D1:76:A4:7F:81:E6:7D:64:F6:96:78:0F:B1:D0:C8:12:0B:2D:04:A9:4A:1A:87:E3:32:AB:49:66:94:B6:0E:5B:02:03:01:00:01*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps* *Policy OID: 2.16.840.1.113733.1.7.44.2* *Policy OID: 0.4.0.194112.1.2*
Subject Key Identifier	*F5:74:48:F4:E1:F6:4C:3F:0B:21:B9:00:F7:25:83:67:05:61:D3:58*
Authority Key Identifier	*FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40*
Subject Alternative Name	*apostolos.apladas@ec.europa.eu*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Extended Key Usage	*id_kp_clientAuth*
Authority Info Access	*http://std-ocsp.trustwise.com* *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/ca.crt*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1E:34:FF:80:C0:3E:03:F8:98:21:8C:5E:99:04:1C:5C:5E:83:14:AC:62:72:2E:07:11:B3:7F:A1:B0:F9:67:43*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*364601280170338855397274057158916865 45*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIBTCCBu2gAwIBAgIQG233GXjL5UvTeIT2PvwMkTANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2lQYWxTaWdnIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeWJhbnRlYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIEIhbmFnZWQgUEsJ
IElnZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVk
IENBIC0gRzMwHhcNMjAwNDA4MDAwMDAwWhcNMjMwNDA4MjM1OTU5WjCCAaIxCzAJBgNVBAYTAkJF
MRwwGgYDVQQKFBNFVVJPUEVBFiBDT01NSVNTSU9OMdRkwFwYDVQRhFBBWQVRCRS0wOTQ5MzgzMzQy
MT0wOwYDVQQLEzRDZX0aWZpY2F0ZSBQcm9maWxlIC0gUXVhbGlmaWVkIENlcnRpZmlpYXRlIC0g
TWVtYmVyMUUwQwYDVQQLExUZXltcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24u
cHQvRUNESUdJVEFMU0lHIY59ycGExfjAgBgNVBAsUGUVudGl0bGVtZW50IC0gRUMgT0ZGSUNJQUwx
KDAmBgkqhkiG9w0BCQEWGWplcm9lbn5yYXRoZUBlYy5ldXJvcGEuZXUxHTAbBgNVBAUTFFBOT0JF
LTU5M0I1NDQ0NzUwLTI3MQwDAYDVQQEFAVSQVRlRTEYMBYGA1UEKhQPSkVST0VOEFSTk9MRCBM
MR0wGwYDVQQLFBRSZW1vdGVRU0NETWFuYWdlbWVudDEcMBwGA1UEAxQVSkVST0VOEFSTk9MRCBM
IFJBVEhFMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6Xu4L2ZrE0heHhD4huf8MTgi
MllyYlovFMV61b96MPAYELPRhaBIVHHF7w082rUdleHZ4zvmDVWtb0b9QGv+kx2KzXQMkOvsH7Sv
CUVrKZzzmwYFNynPMqEmO3XaCEbDY09Fvl5vaGywn1USS5TCFA135+Kpu6cfnK8JOFyTLthjMw
HPvbQOE4gmx07wW2CHwxt2PV/JPmD1aC4ZakkUNwgMCbG3igKRu8+pMVwWpmil3k1SSfcBLZ4gTc
hErFE5OyP6jC1iFkLJcX1r/Lgmv3quQrmaXKilLgYX6XnHajHp3Ay+VtXniMRp9mEjPAdYDMlrFZ
nqH5HYjaFPPI8wIDAQABo8IDGTCCAxUwCQYDVR0TBAIwADBzBgNVHR8EbDBqMGigZqBkhmJodHRw
Ob8vb25zaXRlY3JsLnRydXN0d2lzZS5jb20vRGlnaXRhbFNpZ25DZXJ0aWZpY2Fkb3JhRGlnaXRh
bFF1YWxpZmllZENlcnRpZmlpYXRlRzMvTGF0ZXN0Q1JMLmNybDAOBgNVHQ8BAf8EBAMCBkAwbgYD
VR0gBGcwZTBJBgtghkgBhvhFAQcXAjA6MDgGCCsGAQUFBwIBFixodfHrwczovL3d3dy5kaWdpdGFs
c2lnb5wdC9FQ0RJR0lUQUxTSUdOL2NwczANBgtghkgBhvhFAQcsAjAJBgcEAIvsQAECMB0GA1Ud
DgQWBBQEFGc7bat3ndlp+9HIY8+pkI8zbaTAIBgNVHSMEGDAWgBTTXo5CnCOotfQbjFx8Ozr2dts3
QDAkBgNVHREEHTAbgRlqZXJvZW4uemF0aGVAZWMuZXYyb3BhLmV1MIHImBggrBgEFBQcBAwSB2TCB
1jAVBggrBgEFBQcLAjAJBgcEAIvsSQEBMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwCAYGBACORgEB
MAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGATB9BgYEAI5GAQUwczA2FjBodHRwczovL3d3
dy5kaWdpdGFsc2lnb5wdC9FQ0RJR0lUQUxTSUdOL2Nwcy9kZHATAIBUMDkWM2hfdHBzOi8wd3d3
LmRpZ2lQYWxzaWduL.nB0L0VDREIHSVRBTFNJR04vY3BzL2Rkcf9lbhMCRU4wHQYDVR0lBBYwFAYI
KwYBBQUHAwIGCCsGAQUFBwMEMIGkBggrBgEFBQcBAQSBlzCBlDApBggrBgEFBQcwAYYdaHR0cDov
L3N0ZC1vY3NwLnRydXN0d2lzZS5jb20wZwYIKwYBBQUHMAKGW2h0dHA6Ly9vbnNpdGVjcmwudHJ1
c3R3aXNlLmNvbS9EaWdpdGFsU2lnbkNlcnRpZmlpYWRvcmFEaWdpdGFsUXVhbGlmaWVkQ2VydGlm
aWNhdGVHMy9YS5cnOwDQYJKoZIhvcNAQELBQADggEBAHH5v7PtqFP0Nh5E1503NL9TTmLHF2f
zEf0xF14dpQ/90Sbbn3F1/D7rwX6lyvRPIXvNmb0aN0xQ+y1rjB44znnLdGLFND9gx3Y8BR4edA
R+21xhznjT/6du0g2BKiOmJP/4bl65Cy9mJz5qeHzxXr9Y/W4FUy2m11xQze9/nFdMiD2Yzy/fgs
V9brkF5dIz2yIzE6E/FYaa85M4W770Ep6WlemeilUbDfjws2zDi0gR7sksNzMc3HWVtI0eNf5zj
3HIXxGe9TBG83jm4ppO13K7KEFLlmJdoYDp6zY8x6KNjbFH0N8YoobCG83cO8CUSHczD3PuBQ
VOI0Qu8=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G3*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *JEROEN ARNOLD L RATHE*

Subject OU: *RemoteQSCDManagement*

Subject GIVEN NAME: *JEROEN ARNOLD L*

Subject SURNAME: *RATHE*

Subject SERIAL NUMBER: *PNOBE-592-5444750-27*

Subject E: *jeroen.rathe@ec.europa.eu*

Subject OU: *Entitlement - EC OFFICIAL*

Subject OU: *Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa*

Subject OU: *Certificate Profile - Qualified Certificate - Member*

Subject 2.5.4.97: *VATBE-0949383342*

Subject O: *EUROPEAN COMMISSION*

Subject C: *BE*

Valid from: *Wed Apr 08 02:00:00 CEST 2020*

Valid to: *Sun Apr 09 01:59:59 CEST 2023*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E9:7B:B8:2F:66:6B:13:48:5E:1E:10:F8:86:E7:FC:31:38:22:32:59:72:60:8A:2F:14:C5:7A:D5:BF:7A:30:F0:18:10:B3:D1:85:A0:48:54:71:C5:EF:0D:3C:DA:B5:1D:95:E1:D9:E3:3B:E6:0D:55:AD:6F:46:FD:40:6B:FE:93:1D:8A:CD:74:0C:90:EB:EC:1F:B4:AF:09:45:6B:29:9C:F3:9B:06:05:37:29:CF:32:A1:26:3B:75:EE:08:46:C3:63:4F:45:BE:5E:6F:68:68:F0:9F:55:12:E7:94:FF:08:50:35:DF:9E:06:A5:AE:9C:7E:7F:0A:89:F3:85:C9:32:ED:86:33:30:1C:FB:DB:40:E1:38:82:6C:74:EF:05:B6:08:7C:31:B7:63:D5:FC:93:E6:0F:56:82:E1:96:A4:91:43:70:80:C0:9B:1B:78:A0:29:1B:BC:FA:93:15:C1:6A:66:8A:5D:E4:D5:24:9F:C4:12:D9:E2:04:DC:84:4A:C5:13:94:32:3F:A8:C2:D6:21:64:2C:97:17:D6:BF:CB:82:7B:F7:AA:E4:2B:99:A5:CA:8A:52:E0:61:7E:97:9C:76:A3:1E:9D:C0:CB:E5:6D:5E:78:8C:46:9F:66:12:33:C0:75:80:CC:96:B1:59:9E:A1:F9:1E:D6:1A:14:F3:C8:F3:02:03:01:00:01*

Basic Constraints *IsCA: false*

CRL Distribution Points *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl*

Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps

Policy OID: 2.16.840.1.113733.1.7.44.2

Policy OID: 0.4.0.194112.1.2

Subject Key Identifier *04:14:67:3B:6D:AB:77:9D:D2:29:FB:D1:D3:F3:EA:64:D7:CC:DB:69*

Authority Key Identifier *FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40*

Subject Alternative Name *jeroen.rathe@ec.europa.eu*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_QcSSCD

Extended Key Usage *id_kp_clientAuth*

Authority Info Access

http://std-ocsp.trustwise.com

http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/ca.crt

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B5:F7:9F:E7:98:AA:FF:B5:06:E7:EF:62:FA:F0:E2:6E:E4:73:E8:2F:04:CF:1F:A1:AD:71:F9:A5:94:7A:7F:90*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *152703152656524884086473193861611914911*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIH4DCCBsigAwIBAgIQcuGOs8Fyv7YDW1ZyZ14GnzANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2l0YWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeWJhbnRlYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEsJ
IElnZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZZ24gUXVhbGlmaWVk
IENBIC0gRzMwHhcNMjAwNzA2MDAwMDAwWhcNMjMwNzA2MjM1OTU5WjCCAXoxCzAJBgNVBAYTAkdS
MRwwGgYDVQQKFBNFVVJPUEVBTiBDT01NSVNTSU9OMRkwFwYDVQRhFBBWQVRCRS0wOTQ5MzgzMzQy
MT0wOwYDVQQLEzRDZXJ0aWZpY2F0ZSBQcm9maWxlIC0gUXVhbGlmaWVkIENlcnRpZmlpYXRlIC0g
TWVtYmVyMUUwQwYDVQQLExUZXJtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24u
cHQvRUNESUdJVEFMU0lHIi9ycGExIjAgBgNVBAsUGUVudGl0bGVtZW50IC0gRUMgT0ZGSUNJQUwx
KzApBgkqhkiG9w0BCQEWHGdlb3JnaW9zLmxhcHBhc0BlYy5ldXIvcGEuZXUxDzANBgNVBAQUBkxB
UFBBUzERMAkGA1UEKhQRb0VPLkdlT1MxHTAbBgNVBAsUFFJlb W90ZVFTQ0RNYW5hZ2VzZW50MRgw
FgYDVQQDFA9HRU9SR0lPUyBMQVBQQVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDL
mkGUsomW+QoxIwY+nH5XRW6DDvVXoDYJnM4a0R/sGmlAQgosfa8yrGmVSWxDRoXxUAlNKzXd1yGm
Pt6gSW6rMIWyZsxIldNAvYKTJdKDCSGRtScit0hrbkrCTydOfML7E+R5gTUTa02kRuwg08ZrwQ7B
5rvOoJVBCZMSZBrPp8hlt8qZHIN8fMEByPbwR5ia70EPXts8Xc64z6PESX6ow5gok+WgH2980S
EVuB9HJN1BtcBsyiGpVjZmRpwsprEzkYEcUoLxv1THXVdwVQloq9yrG4HjXgxbv14LGE85vgUvl4
8wk3D5wb/RaVO8k0V9gle4aa0r4tOHekb/mdAgMBAAGjggMcMIIDGDAJBgNVHRMEAjAAMHMGA1Ud
HwRsMGowaKBmoGSGYmh0dHA6Ly9vbnNpdGVjcmwudHJ1c3R3aXNlLmNvbS9EaWdpdGFsU2lnbkNl
cnRpZmlpYWRtcmFEaWdpdGFsUXVbbGlmaWVkQ2VydGlmaWNhdGVlHMy9MYXRlc3RDUkwuY3JlMA4G
A1UdDwEB/wQEAwIGQDBuBgNVHSAEZzBlMEkGC2CGSAGG+EUBBxcCMDowOAYIKwYBBQUHAgEWLGh0
dHBzOi8vd3d3LmRpZ2l0YWxzaWduLnB0L0VDRElHSVRBTFNJR04vY3BzMA0GC2CGSAGG+EUBByw C
MAkGBwQAi+xAAQIwHQYDVR0OBBYEFI8V/EJXbRFSHE3lMSwoiF/2F2wMMB8GA1UdIwQYMBaAFPtc
jkCef0b99BuMXHw7GKvZ2fdAMCxGA1UdEQQgMB6BHGdlb3JnaW9zLmxhcHBhc0BlYy5ldXJvcGEu
ZXUwgeYGCCsGAQUFBwEDBIHZMIHWMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQEwFQYIKwYBBQUHCwIw
CQYIBACL7EkBAjAIBgYEAI5GAQEwCAYGBACORgEEMBMGBgQAjkYBBjAJBgcEAI5GAQYBMH0GBgQA
jkYBBTBzMDYWMGh0dHBzOi8vd3d3LmRpZ2l0YWxzaWduLnB0L0VDRElHSVRBTFNJR04vY3BzL2Rk
eBMCUFQwORYzaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdJVEFMU0lHTi9jcHMvZGRw
X2YuEwJFTjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwgaQGCCsGAQUFBwEBBIGXMIGU
MCkGCCsGAQUFBzABhh1odHRwOi8vc3RkLW9jc3AudHJ1c3R3aXNlLmNvbTBnBggrBgEFBQcwAoZb
aHR0cDovL29uc2l0ZWNybC50cnVzdHdpc2UuY29tL0RpZ2l0YWxTaWduQ2VydGlmaWNhZG9yYURp
Z2l0YWxRdWFsaWZpZWRDZXJ0aWZpY2F0UczL2NhLmNydDANBgkqhkiG9w0BAQsFAAOCAQEAd9KF
wXgDLoL NjXxhovrQ7KzzzwNJywPlNZzjQ+TxSW+uHGsttR6jM167pUL kjQEkm7mKo3RdiGS+MmQ70
HTSgWbOMq8IpbAXSb8B4JT8S8PXsKQ2qoEd2szbJ9UCPm+vJ0+C9PI7ISD+yOJtIz+q15qvMp4jO
BLCmn1k/geTZC3hgK90b96HiDEcXhhpzGJgHOA1R3Scqj7UKklUyt4xYuBAAbcSLUZ159tn0mAEX
YUrYafjdeWTILe7MEWIBwPNVcMK2MnvScuzibED99JKGevHnY6GrE+4vmqn4Y0NyrNu5MbPO12Xw
eDACPzZQIzUbmJsy21LpyVbCWgFNf4PFJA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G3*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *GEORGIOS LAPPAS*

Subject OU: *RemoteQSCDManagement*

Subject GIVEN NAME: *GEORGIOS*

Subject SURNAME: *LAPPAS*

Subject E: *georgios.lappas@ec.europa.eu*

Subject OU: *Entitlement - EC OFFICIAL*

Subject OU: *Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa*

Subject OU: *Certificate Profile - Qualified Certificate - Member*

Subject 2.5.4.97: *VATBE-0949383342*

Subject O: *EUROPEAN COMMISSION*

Subject C: *GR*

Valid from: *Mon Jul 06 02:00:00 CEST 2020*

Valid to: *Fri Jul 07 01:59:59 CEST 2023*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:9A:41:94:B2:89:96:F9:0A:31:23:06:3E:9C:7E:57:45:6E:83:0E:F5:57:A0:36:09:9C:CE:1A:D1:1F:EC:1A:69:40:42:0A:2C:7D:AF:32:AC:69:95:49:6C:43:46:85:F1:50:09:4D:2B:35:DD:D7:21:A6:3E:2E:A0:49:6E:AB:30:85:B2:66:CC:48:95:D3:40:BD:82:93:25:D2:83:09:21:91:7D:27:22:B7:48:6B:6E:4A:C2:4F:27:4E:7C:C2:FB:13:E4:79:81:35:13:6B:4D:A4:46:EC:20:D3:C6:73:C1:0E:C1:E6:BB:CE:A0:88:D5:04:26:4C:E5:9D:81:AC:FA:52:84:1F:FC:A9:91:C8:35:B7:CC:10:1C:8F:6F:0F:39:89:AE:F4:10:F5:E1:4B:C5:DC:EB:8C:FA:3C:4E:57:EA:8C:39:82:89:3E:5A:01:F6:F7:C9:52:11:5B:81:F4:72:4D:D4:1B:5C:06:CC:A2:1A:95:63:66:64:69:C2:CA:6B:13:39:18:11:C5:28:2F:1B:F5:4C:75:D5:77:05:50:22:8A:BD:CA:B1:B8:1E:35:E0:C5:BB:F5:E0:B1:84:F3:9B:E0:52:F9:78:F3:09:37:0F:9C:1B:FD:16:95:3B:C9:34:57:D8:25:7B:86:9A:D2:BE:2D:38:77:A4:6F:F9:9D:02:03:01:00:01

Basic Constraints

IsCA: false

CRL Distribution Points

http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl

Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps

Policy OID: 2.16.840.1.113733.1.7.44.2

Policy OID: 0.4.0.194112.1.2

Subject Key Identifier

8F:15:FC:42:57:85:11:52:1C:4D:E5:31:2C:28:88:5F:F6:17:6C:0C

Authority Key Identifier

FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40

Subject Alternative Name

georgios.lappas@ec.europa.eu

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_QcSSCD

Extended Key Usage

id_kp_clientAuth

Authority Info Access

http://std-ocsp.trustwise.com

http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/ca.crt

Key Usage:

nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

17:F7:71:1F:C9:CB:70:2A:35:CD:1D:DF:03:FF:13:0C:6D:D0:2A:4E:56:F7:CB:8C:D5:C9:AD:CF:52:EA:3F:95

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:

3

Serial Number:

163467828690131502343104343442326302118

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIH9jCCBt6gAwIBAgIQevrCNQpIXiCh355eXjwtpjANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2lUYWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeWJhbnRlYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEsJ
IEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZZ4gUXVhbGlmaWVk
IENBIC0gRzMwHhcNMjAwOTI1MDAwMDAwWhcNMjMwOTI1MjM1OTU5WjCCAZAxCzAJBgNVBAYTAlJP
MRwwGgYDVQQKFBNFVVJPUEVBTiBDT01NSVNTSU9OMRkwFwYDVQR6FBBWQVRCRS0wOTQ5MzgzMzQy
MT0wOwYDVQQLEzRDZXJ0aWZpY2F0ZSBQcm9maWxlIC0gUXVhbGlmaWVkIENlcnRpZmlpYXRlIC0g
TWVtYmVyMUUwQwYDVQQLExUZXJtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24u
cHQvRUNESUdJVEFMU0lHT19ycGExfjAgBgNVBAsUGUVudGl0bGVtZW50IC0gRUMgT0ZGSUNJQUwx
KzApBgkqhkiG9w0BCQEWHGFkcmlhbi5jcm9pdG9ydUBlYy5ldXvcGEuZXUxETAPBgNVBAQUCENS
T0lUTTJVMRowGAYDVQQgFBFDT05TVEFOVEIOLUFEUkltRTJEdMB8GA1UECxQUIm Vtb3RlUVNDRE1h
bmFnZWllbnQxIzAhBgNVBAMUGkNPTlNUQU5USU4hQURSSUFOIENST0lUT1JVMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAutg6Rc Trmbtc PoxGSoMC1O5+151zAdaw21AklQOnkEMkC8aa
5d4utJ3nfiOVIGRd6fFGu8hb8osuxzYEb6ycz5y/OiRVUkr96Gj7LzEv/lIFdnIAQMmr+FATvolw
+Q8uld8WJlaVW04/b+DrEPmbXmx8AoNrzSTcIcQnmn5gZy5jaDT/fD3cIYpcdkAE9XaiLmfv4Lnv
OvnAHuIVcY+LXvrdLVFtSCn7Y37b0GwVWTUCkvhwY1xoJm1fgM/OLxfN0SFBHFihRPD2qPHdnu/C
xH4/CLvEZM2ljJAPgUxlwhJy32luiifadTAeHavzNM1ND/sQnKypcDH1WiaeMPsw4QIDAQABo4ID
HDCCAxgwCQYDVR0TBAIwADBzBgNVHR8EbDBqMGigZqBkhmJodHRwOi8vb25zaXRlY3JsLnRydXN0
d2lzZSj b20vRGlnaXRhbFNpZ2SDZXJtaWZpY2Fkb3JhbRGlnaXRhbFF1YWkpZmlIZENlcnRpZmlj
YXRlRzMvTGF0ZXN0Q1JMLmNybDAOBgNVHQ8BAf8EBAMCBkAwbgYDVR0gBGcwZTBJBgtghkgBhvhF
AQcXAj A6MDgGCCsGAQUFBwIBFixodHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RJR0lUQUx1
SUdOL2NwczANBgtghkgBhvhFAQcsAjAJBgcEAIvsQAECMB0GA1UdDgQWBBRF9L g2cLhB8QApjl2q
jMcSz7Q3JDAJBgNVHSMEGDAWgBT7Xo5CuCOoIQbjFx8Oxu2dn3QDAnBgNVHREEIDAcgRsbZHJp
YW4uY3JvaXRvcnVAZWMuZXVvb3BhLmV1MIHImBggrBgEFBQcBAwSB2TCB1jAVBggrBgEFBQcLAjAJ
BgcEAIvsSQEBMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwCAYGBACORgEBMAgGBgQAjkYBBDATBgYE
AI5GAQYwCQYHBACORgEGATB9BgYEAI5GAQUwczA2FjBodHRwczovL3d3dy5kaWdpdGFsc2lnbi5w
dC9FQ0RJR0lUQUx TSUdOL2Nwcy9kZHJATAIBUMIDkWM2l6IdHBzOi8vd3d3LmRpZ3lYWxzaWduLnB0
L0VDREIHSVRBTFNJR04v YHzL2Rkcf9lbhMCRU4wHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUF
BwMEMIGkBggrBgEFBQcBAQSBlzCBlDApBggrBgEFBQcwAYYdaHR0cDovL3N0ZC1vY3NwLnRydXN0
d2lzZSj b20wZwYIKwYBBQUHMAKGW2h0dHA6L y9vbnNpdG Vjcmwudf1J1c3R3aXNlLmNvbS9EaWdp
dGFsU2lnbkNlcnRpZmlj YWRvcmFEaWdpdGFsUXVhbGlmaWVkQ2VydGlmaWNhdGVHMy9YS5jcnQw
DQYJKoZIhvcNAQELBQADggEBAF36+WqrF09d+DnaWN6u+3I+L5GzNZozQ7zqgJBgECDuuM5ZD1Yi
u6a8GlUvnwVFQVJ3jahn7wF0NtKsl4gx43xcuWL4npatQ6Lptt5Zhx9r7e8/gxCwTqSI3wM3obzj
0VS2oXNqsbkt4yho+tmdyrbUv43vmrFzV0e95ULtdPVz9ilImd6IBPkMA2ZPZJlufa63loSOK54
By40FNX3NIUvsrd9Op8BN5kgeFzuLTibZA5GSF/hfgbECyDlNOcSRDRNc8qN58S91VgGfLRBvZRg
WlyNqZl9ifpzc+8qM+tiHkocQf7mFuhKcENmN+EE+VXKlqPjovE5z7QKq0OOmPZw=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G3*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *CONSTANTIN-ADRIAN CROITORU*

Subject OU: *RemoteQSCDManagement*

Subject GIVEN NAME: *CONSTANTIN-ADRIAN*

Subject SURNAME: *CROITORU*

Subject E: *adrian.croitoru@ec.europa.eu*

Subject OU: *Entitlement - EC OFFICIAL*

Subject OU: *Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa*

Subject OU: *Certificate Profile - Qualified Certificate - Member*

Subject 2.5.4.97: *VATBE-0949383342*

Subject O: *EUROPEAN COMMISSION*

Subject C: *RO*

Valid from: *Fri Sep 25 02:00:00 CEST 2020*

Valid to: *Tue Sep 26 01:59:59 CEST 2023*

Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:D8:3A:45:C4:EB:99:BB:5C:3E:8C:46:4A:83:02:D4:EE:7E:D7:9D:73:01:D6:B0:DB:50:24:95:03:A7:90:43:0A:0B:C6:9A:E5:DE:2E:B4:9D:E7:7E:24:15:20:64:5D:EA:D1:46:BB:C8:5B:F2:8B:2E:C7:36:04:6F:AC:9C:CF:9C:BF:3A:24:55:52:4A:FD:E8:68:BB:2F:31:2F:FE:52:05:76:E2:00:40:C9:AB:F8:50:13:BE:89:70:F9:00:6E:21:DF:16:24:96:95:5B:4E:3F:87:E0:EB:10:F9:9B:5E:6C:7C:02:83:6B:AD:24:DE:25:C4:1A:9E:6E:60:67:2E:63:68:34:FF:7C:3D:DC:25:8A:5E:76:40:04:F5:76:A2:2E:67:EF:E0:B9:EF:3A:F9:C0:1E:E2:15:79:8F:8B:5E:FA:DD:2D:51:6D:48:29:FB:63:7E:DB:D0:6C:15:59:35:02:92:F8:70:63:5C:68:26:6D:5F:80:CF:CE:2F:17:CD:D1:21:41:1C:58:A1:44:F0:F6:A8:F1:DD:9E:EF:C2:C4:7E:3F:08:BB:C4:64:CD:88:8C:90:0F:81:4C:48:C1:B2:72:DF:62:2E:88:87:DA:75:30:1E:1D:AB:F3:34:CD:4D:0F:FB:10:9C:AC:A9:78:31:F5:5A:26:9E:30:FB:30:E1:02:03:01:00:01*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps* *Policy OID: 2.16.840.1.113733.1.7.44.2* *Policy OID: 0.4.0.194112.1.2*
Subject Key Identifier	*45:F4:B8:36:70:B8:41:F1:00:29:8E:5D:AA:8C:C7:92:CF:B4:37:24*
Authority Key Identifier	*FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40*
Subject Alternative Name	*adrian.croitoru@ec.europa.eu*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Extended Key Usage	*id_kp_clientAuth*
Authority Info Access	*http://std-ocsp.trustwise.com* *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/ca.crt*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*56:F7:05:C2:E4:6C:B3:5A:78:B2:7A:7A:13:64:C7:33:FB:82:26:D9:6F:F0:1E:8E:2F:02:10:31:36:A8:67:51*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*362671125803220245397713982254227056881701192273*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHLjCCBRagAwIBAgIUP4a8WPhZN++7VkfYyuAcDGmTglEwDQYJKoZIhvcNAQELBQAwczELMAkG
A1UEBhMCQkUxGTAXBgNVBGEMEESU1JLFTA1Mzc2OTgzMTgxIDAzBgNVBAoMF1F1b1ZhZGlsIFRy
dXN0bGluayBCVkJBMScwJQYDVQQDDB5RdW9WYWRpcyBCZWxnaXVtIEIzc3VpbmcgQ0EgRzIwIHcN
MjEwMTIxMDg0ODM4WhcNMjQwMTIxMDg1ODAwWjCBwDELMAkGA1UEBhMCQkUxLDAqBgNVBAsMI0Rp
cmVjdG9yYXRlLUdlbmVyYWwgZm9yIEluZm9ybWF0aWNzMRkwFwYDVQRhDBBOVEJCRS0wOTQ5Mzgz
MzQyMDUwSAYDVQQKDEFDT01NSVNTSU9lIERFIEwnVU5JT04gRVVSTTBFRUS0RSAtIENPTUUtNJ
RSBWQUdgREEgRVVST1BFU0UgVU5RTEcMBoGA1UEAwwTRXVyb3B1YW4gQ29hbWIzc2hbjCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMCq40SQWaqRkbc5nsdPjLKyxghYzBLJCmeN3/nd
D5mMzhy9tsP8WOpsfi8CnMD5tasEEmSSFj73DQ+sL9PIyfmLzBJVhuCyzwKpDiFAhAa+ec/LTyVR
a6+oCh91SZUcPDVXpC0GA3t6WS0pCgrIJNkZequ2yIWUXuyVOACYmkxmWhWnGe7LRaLvx80PC10Q
ERL2BzV+mKb2tQylUjnbPPf8bu9LG9EwCvSSXv0tb4rKUC+IlcxuYsu7dNvfw9UHDBmu5452c3O
18N5+GSI9uiEmOI8s++ibubn61RskePhk3ISURPGIAeDKV9pCZezBGysq5lINkC1C4AtYS2eKFcC
AwEAAaOCAmowggJmMB8GA1UdIwQYMBaAFIfJvDGXEnpzu37APUVRtAEllVGrMHcGCCsGAQUFBwEB
BGswaTA4BggrBgEFBQcwAoYsaHR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmFsLmNvbS9xdmJlY2Fn
Mi5jcnQwLQYIKwYBBQUHMAGGIWhldHAtLy91dy5vY3NwLnF1b3ZhZGlzZ2xvYmFsLmNvbTBaBgNV
HSAEUzBRMEQGCisGAQQBvlgBgxAwNjA0BggrBgEFBQcCARYoaHR0cDovL3d3dy5xdW92YWRpc2ds
b2JhbC5jb20vcmVwb3NpdG9yeTAJBgcEAIvsQAEDMCkGA1UdIQQiMCAGCCsGAQUFBwMCBggrBgEF
BQcDBAYKKwYBBAGCNwoDDDCBiwYIKwYBBQUHAQMEfzB9MBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIw
CAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGAjA7BgYEAI5GAQUwMTAvFilo
dHRwczovL3d3dy5xdW92YWRpc2ds2JhbC5jb20vcmVwb3NpdG9yeRMCZW4wOwYDVR0fBDQwMjAw
oC6gLIYqaHR0cDovL2NybC5xdW92YWRpc2dsb2Jhbc5jb20vcXZiZWNhZzluY3JsMB0GA1UdDgQW
BBQspnrB2Vq7SM99egtZxs2jZv1QOjAOBgNVHQ8BAf8EBAMCBsAwEwYKKoZIhvcvAQEJAgQFMAMC
AQEwNAYKKoZIhvcvAQEJAQQmMCQCAQGhMCQCAQGGH2Ih0dHA6Ly90cy5xdW92YWRpc2dsb2Jhbc5jb20vYmUw
DQYJKoZIhvcNAQELBQADggIBACGQDYsjrM3nsKSpWISqzBIZOkvuphSLNhv5o5V1W+muYLtXYH
/fMadrP0+K2X5XB5e+8yMw4Sbrvxv4LRR/CQ2WX03KjYGcqdcIUAH+A/8phwA7eLyKd3ip8k8ukT
9kUKMJxbqVRSO8x2vOIAM9VFirOenOf+MutFDSaNKIJKt+PDhcSxDyzjs2MRKHAJcTCs23T8IB6+
Qvw3uKUjmVg4MTLFvWpL8bvMXX7QUyvsScsKUCns918hHA4Ett7fxdWXJFFJuuculChJIf8jbXQ
Q/8SAueccPyADnJn0C4uGNUzc9/DWqMSMMytFwGet0pQb0/pukdmNc3saiSUQr4+vybkCHKMD27c
ak9buDO7cu5ybKEuLCERTga2QvbGSeiFAa6KuyPGY1Ad9AOuz5KPyyfVG0h31FvNL0MnAib1IpZr
7mPQgWOsEX9jpgQXoE2Rlh11yydTiKwmyTTrp/uMOJp+6UD06IdgPkHmqnqaKkqzGu6RKiHLqYWX5
qhWx0EatHQ0YY+92B03cDTLMgjPHKY+wN6qPfetz0oQNmort+G2HINxb9P+Q43sqMjXpQY/I3YmM
0VBmcYWUon11BOunvnGOCVVPB0QFKU6K17r69li1CmA7KgK7In2o/jb8BupWUPGcrj++MkkrFDS0T
6tmNH9ZDteyO3dSyOcl1IHcs

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *QuoVadis Belgium Issuing CA G2*

Issuer O: *QuoVadis Trustlink BVBA*

Issuer 2.5.4.97: *NTRBE-0537698318*

Issuer C: *BE*

Subject CN: *European Commission*

Subject O: *COMMISSION DE L'UNION EUROPEENNE - COMMISSIE VAN DE EUROPESE UNIE*

Subject 2.5.4.97: *NTRBE-0949383342*

Subject OU: *Directorate-General for Informatics*

Subject C: *BE*

Valid from: *Thu Jan 21 09:48:38 CET 2021*

Valid to: *Sun Jan 21 09:58:00 CET 2024*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C0:AA:E3:44:90:59:AA:91:91:B7:39:9E:C7:4F:8C:B2:B2:C6:08:58:CC:12:C9:0A:67:8D:DF:F9:DD:0F:99:8C:CE:1C
:BD:B6:C3:FC:58:EA:6C:7E:2F:02:9C:C0:F9:B5:AB:04:12:64:B9:16:3E:F7:0D:0F:AC:2F:D3:C8:C9:F9:8B:CC:12:55:86:E0:B2:CF:02:A9:0E:21:40:84:06:BE:79:CF:CB:4F:25:51:6B:AF:A8:0A:1F:75:F1:95:1C:3C:35:57:A4
:2B:46:03:7B:7A:59:2D:29:0A:0A:C8:24:D9:19:7A:AB:B6:C8:85:94:67:18:B2:54:E0:02:62:69:31:99:68:56:9C:67:BB:2D:16:8B:BF:CD:0F:08:8D:10:11:12:F6:07:35:7E:98:A6:F6:B5:0C:A5:52:98:4F:3C:8F:21:77:D2:C6:F4:
4C:02:BD:24:97:BF:4B:5B:E2:B2:B5:0B:E9:48:73:1B:98:B2:E8:BB:74:DC:9F:C3:D5:07:0C:19:EE:23:9E:39:D9:CD:CE:D7:C3:79:F8:64:88:F6:E8:84:98:E2:3C:B3:EF:9F:6E:E6:E7:EB:54:6C:91:E3:E1:93:72:12:51:13:C6:2
0:07:83:29:5F:69:09:97:B3:04:6C:AC:AB:92:25:36:40:B5:0B:80:2D:61:2D:9E:28:57:02:03:01:00:01

Authority Key Identifier *87:C9:BC:31:97:12:7A:73:BB:7E:C0:3D:45:51:B4:01:25:95:51:AB*

Authority Info Access

http://trust.quovadisglobal.com/qvbecag2.crt

http://uw.ocsp.quovadisglobal.com

Certificate Policies

Policy OID: 1.3.6.1.4.1.8024.1.400

CPS pointer: http://www.quovadisglobal.com/repository

Policy OID: 0.4.0.194112.1.3

Extended Key Usage *id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_QcSSCD

CRL Distribution Points

http://crl.quovadisglobal.com/qvbecag2.crl

Subject Key Identifier

2C:A6:7A:C1:D9:5A:BB:48:CF:7D:7A:0B:59:C6:CD:A3:66:FD:50:3A

Key Usage:

digitalSignature - nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

F7:E8:E4:E5:54:FB:7C:7A:8F:6F:36:0E:0C:A2:F5:9D:46:6C:8F:95:39:A2:59:63:F5:ED:37:E9:05:F0:C7:97

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:

3

Serial Number:

602137478369718753674691090226768309702106444 86

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHQTCCBSmgAwIBAgIUCowT7Q98oPLpaLF0FnUX3eobcgYwDQYJKoZIhvcNAQELBQAwczELMAkG
A1UEBhMCQkUxGTAXBgNVBGEMEESUUkJFLTA1Mzc2OTgzMTgxIDAeBgNVBAoMF1F1b1ZhZGlzIFRy
dXN0bGluayBCVkJBMScwJQYDVQQDDB5RdW9WYWRpcyBCZWxnaXVtIEIzc3VpbmcgQ0EgRzIwHhcN
MjEwMTIxMDg0ODIzWhcNMjQwMTIxMDg1ODAwWjCBtzELMAkGA1UEBhMCQkUxPzA9BgNVBAsMNkRH
IGZvciBDb21IdW5pY2f0aW9ucyBOZXR3b3JtcywgQ29udGVudCBhbmQgVGVjaGS0bG9neTEZMBcG
A1UEYQwQTIRSQkUtMDk0OTM4MzM0MjFKMEgGA1UECgxBQ09NTUJITU0lPTiBERSBMJ1VOSU9OIEVV
Uk9QRUVOTkUgLSBDT01NSVNTSUUgVkFOIERFIEVVUk9QRVNFIFVOSUUxHIDAaBgNVBAMME0V1cm9w
ZWFuIENvbW1pc3Npb24wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDfD1bnPz0vyl0g
xH+YcUEyssxJTWyXm1ZSjXSTOoR36yu+FvE11YBTq7CGA2JNUxKdOPgF+MZxj9vOoMwqR1+cbP
DNzXsdzlNLZCDy3mrPt3hfqmjhmqmwwXSQnO2+uDce+BYGXL74oWnqJTc+GT6SjYQMyeXyyff1J
U4pC+QL53tcpcNf7dO5EJzHAfLDp8HILebtafvWAQA9+Psf3BT/0lHQZ1nqnyMfjBntCBG6/Cj2m
tM44vIdCKtRDdGno7MT5IkTvwoIcEA5Lupbdu9sadHsJ7i4iOub8QshIJbjHqP7n7q+OsN5RX5X/b
mIG03j7Yr+DfwCKwE4cKsZHAgMBAAGjggIqMIICZjAJBgNVHSMEGDAWgBSHybwxIc36c7t+wD1F
UbQBJZVRqzB3BggrBgEFBQcBAQRtMGkwOAYIKwYBBQUHMAKGLGh0dHA6Ly90cnVzdC5xdW92YWRp
c2dsb2JhbC5jb20vcXZiZWNhZzIuY3J0MC0GCCsGAQUFBzABhiFodHRwOi8vdXcub2NzcC5xdW92
YWRpc2dsb2JhbC5jb20wWgYDVR0gBFMwUTBEBgorBgEEAb5YAYMQMDYwNAYIKwYBBQUHAgEWKGh0
dHA6Ly93d3cucXVvdmFkaXNnbG9YWwuY29tL3JlcG9zaXRvcnkwCQYHBACLf7EABAzApBgNVHSUE
IjAgBggrBgEFBQcDAgYIKwYBBQUHAwQGCisGAQQBgjcKAwwwgYsGCCsGAQUFBwEDBH8wfTAVBggr
BgEFBQcLAjAJBgcEAIvsSQECMAgGBgQAjkYBATAIBgYEAI5GAQQwEwYGBACORgEGMAkGBwQAjkYB
BgIwOwYGBACORgEFMDEwLxYpaHR0cHM6Ly93d3cucXVvdmFkaXNnbG9YWwuY29tL3JlcG9zaXRv
enkTAmVuMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwucXVvdmFkaXNnbG9YWwuY29tL3F2
YmVjYWcyLmNvbDAdBgNVHQ4EFgQUSikDpwxZxh51U75EfhdERrD98wDgYDVR0PAQH/BAQDAgbA
MBMGCiqGSIb3LwEBCQIEBTADAgEBMDQGCiqGSIb3LwEBCQEEJjAkAgEBhh9odHRwOi8vdHMucXVv
dmFkaXNnbG9YWwuY29tL2JlMA0GCSqGSIb3DQEBCwUAA4ICAQCWLVCxzkKy/s+8kRvxCPvTlExl
WkNGszhCO+PXsh1UgWMdJCpc33OzL1GegNMSL9f3Hw6gqjXV+mJqtTmvrP1ZvXCagv2LRLeyxSYA
jIVjwYkaradydxBS8Ot86OytA0OIs1UruPe0lCIb6zBKwqx7L vXotk7XvPYQo0HtP57pCqIp4MIi
NEpGeW3gRwFq8IBQceeO3k009ad+tuTSB51+o4t/7kEd//6voViy7d/EmlOgUZzXsJ24NV4pFAmy
c2FlkEvYOqw8YvEsOV2hluvcG3wmkMEF/SY4X+kvpw+Ph7JQdWpWGlozzAFVppkIIrSM2Sxw2QXF
QZWwah210HhVY0Ax4VkQbRJQNYmFWVizxPONWtc3PIfMz3/TvD9ZbExfIoQcVYXZPmtK2aQjG3C
H2bKcefx518YdR169au8yNKsPvILaRa1k7Qv6Hv8iE3GiQtmszDwnQHIGrbxdfi306gOFI8UQcty
lI2YkG6J/uTnYiibeDoHK6wBo3BfCJQ2X7/Iab3971k1wSCwe39w4x3Xw72HL9E3czRkcfpg+uT
xt5jSJ7HL7BRdMD34ysjQ4gOV8h6NU4z+QQ3W4sZTQkFqHGHKZKt2dTrCjhE+I1hULvo4274heBr
/5F0DBAXRi9lHBCBUV5iJDm90bxjHjKuvj893WLEFW3WPkWlRw==

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

QuoVadis Belgium Issuing CA G2

Issuer O:

QuoVadis Trustlink BVBA

Issuer 2.5.4.97:

NTRBE-0537698318

Issuer C:

BE

Subject CN:

European Commission

Subject O:

COMMISSION DE L'UNION EUROPEENNE - COMMISSIE VAN DE EUROPESE UNIE

Subject 2.5.4.97:

NTRBE-0949383342

Subject OU:

DG for Communications Networks, Content and Technology

Subject C:	*BE*
Valid from:	*Thu Jan 21 09:48:23 CET 2021*
Valid to:	*Sun Jan 21 09:58:00 CET 2024*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:ED:0F:56:E7:3F:3D:2F:C8:8D:20:C4:7F:98:7B:F5:04:CA:CB:31:D5:35:B2:5E:64:F6:4A:35:FC:4F:4A:11:DF:AC:AE:F8:5B:C4:23:56:01:EE:AE:C2:18:0D:89:35:4C:4A:74:E3:E0:16:2E:0C:67:18:FD:BC:EA:0C:C2:A4:75:F9:C6:CF:0C:DC:D7:B1:DC:C8:34:B6:42:0F:2D:E6:AC:FB:77:85:FA:A6:8A:38:66:AA:6C:30:5D:24:27:3B:6F:AE:0D:C7:BE:05:81:97:2F:BE:28:5A:7A:89:4D:CF:86:4F:A4:A3:61:03:32:79:7B:F2:7D:FD:49:53:8A:42:F9:02:F9:DE:D7:29:70:D7:FB:74:EE:44:27:31:C0:7C:B0:E9:F0:72:0B:79:BB:5A:7E:F5:80:40:0F:7E:3E:C7:F7:05:3F:F4:94:74:19:D6:7A:A7:C8:C7:E3:06:7B:42:04:6E:BF:0A:3D:A6:B4:CE:38:BE:57:42:2A:D4:43:74:69:E8:EC:C4:F9:97:14:EF:C2:82:1C:10:0E:4B:BA:96:DD:BB:DB:2E:74:7B:09:4F:88:8E:B9:BF:10:B2:12:37:6E:31:EA:3F:B9:FB:AB:E3:AC:37:94:57:E5:7F:DB:98:81:B4:DF:78:FB:62:7F:83:7F:00:8A:C0:4E:1E:2A:C6:47:02:03:01:00:01*
Authority Key Identifier	*87:C9:BC:31:97:12:7A:73:BB:7E:C0:3D:45:51:B4:01:25:95:51:AB*
Authority Info Access	*http://trust.quovadisglobal.com/qvbecag2.crt* *http://uw.ocsp.quovadisglobal.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.8024.1.400* *CPS pointer: http://www.quovadisglobal.com/repository* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
CRL Distribution Points	*http://crl.quovadisglobal.com/qvbecag2.crl*
Subject Key Identifier	*4A:22:89:3F:0C:59:BE:58:B9:D5:4E:F9:11:F8:5D:11:1A:C3:7F:DF*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*91:27:BC:BD:E1:58:6E:02:DB:9D:71:49:88:13:9E:A2:80:5F:21:DC:08:83:48:A7:E4:FE:62:69:89:51:38:BD*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*212676479325594043390357602242635120 27*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIG7zCCBNegAwIBAgIQEAAAAAAnuXHXttK9Tyf2zANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQG
EwJCRTERMA8GA1UEBxMIQmJlc2NlbHMxHDAaBgNVBAoTE0NlcnRpcG9zdCBQLJYuL1MuQS4xEzAR
BgNVBAMTCkNpdGlleZW4gQ0ExDzANBgNVBAUTBjIwMTgwMzAcFwthxODA2MDEyMjA0MTIaFwtyODA1
MzAyMzU5NTlaMHAxCzAJBgNVBAYTAkJFMSMwIQYDVQQDExpQYXRyaWNrIEtyZW1lciAoU2lnbmF0
dXJlKTEPMA0GA1UEBBMGS3JlbWVyMRUwEwYDVQQqEwxQYXRyaWNrIEplYW4xFDASBgNVBAUTCzcy
MDIwMzI5OTcwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AAMIIBCgKCAQEAr7g7VrIdY4asS4LPOg7
uPH5mIzaVMOwFb/8YOW+9YMHIzV5dJAzeTKvbLGS54Pk6Kd2E+h18fIRonp70Gv2+jtkPk7ZQ
kfez0ycuAbLXiNx2S7fc5GG9L GJaIDJgBgTQuQm1aDVLDQ653mqRStAO+gEf8vs4zRESL3MkYXAU
q+S/WocEaGplheNVAF3iPSkvEe3LvUjF/xXHWF4aMvqGK6kXGseaTcn9hgTbceuW2PAiEr+eDTNc
zkwGBDFXwzmnGFPMRcez3ONk/jIKhha8TylDSIl/MX3ODh0dU3yvJEKPIfUJixBPehxMJMwWxTjFb
NuCK7t8qT2iIS4VQIDAQABo4ICpzCCAossHwYDVR0jBDgwFoAU2TQbPpCIW3hu7++R0z4Aq3j
L1QwcwYIKwYBBQUHAQEEZzBlMDkGCCsGAQUFBzAChi1odHRwOi8vY2VydHMuZWlkLmJlbGdpdW0u
YmUvY2l0aXplbjIwMTgwMy5jcnQwKAYIKwYBBQUHMAGGHGh0dHA6Ly9vY3NwLmVpZC5iZWxnaXVt
LmJlLzlwggEjBgNVHSAEggEaMIIBFjCCAQcGB2A4DAEBAgEwgfswLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0 b3J5LmVpZC5iZWxnaXVtLmJlMIHIKBggrBgEFBQcCAjCBvQyBukdlYn1laWsgb25k
ZXJ3b3JwZW4gYWFulGFhbnNwcmFrZWxpamtoZWlkc2JlcGVya2luZ2VuLCB6aWUgQ1BTIC0gYXNh
Z2Ujec291bWlzIMOgIGRlcyBsaW1pdGF0aW9ucyBkZSByZXNwb25zYWJpbGl0w6ksIHZvaXIgQ1BT
IC0gYmVyd2VuZHVuZyB1bnRlcmxpZWd0IEhhZnR1bmdzYmVzY2hyw6Rua3VuZ2VuLCBnZW3DpHNz
IENQIzAJBgcEAIvsQAECMDKGA1UdHwQyMDAwLqAsoCqGKGh0dHA6Ly9zcmwuZWlkLmJlbGdpdW0u
YmUvZWlkYzIwMTgwMy5jcmwwDgYDVR0PAQH/BAQDAgZAMBMGA1UdJQQMMAoGCCsGAQUFBwMEMGwG
CCsGAQUFBwEDBGAwXjAIBgYEAI5GAQEwCAYGBACORgEEMDMGBgQAjkYBBTApMCcWIWh0dHBzOi8v
cmVwb3NpdG9yeS5laWQuYmVsZ2llbS5iZRMCZW4wEwYGBACORgEGMAkGBwQAjkYBBgEwDQYJKoZI
hvcNAQELBQADggIBACBY+0LbM7BryzXWkIDUb9LK1+cIDVboPg+lN1Es1IAEoxV4y9zaXUWLco9t8
M5WfIcWFfDxyfatLedka2GurS1t8OJknDwLLyofE1r2Db9VrdG+jtST+j/TmJHAX3yNWjn9dsj
iGQQuTJccce86rlzbGdUqjFTt5mGMm4zyll/wKy6XiDKiZT8cFcOTevsl+l/vxiLiDnghOwTztVZh
mWExcHG9ypqMFYmluclHQ0SFZre8mv3c7DI+VhqV/sY9xLERK3Flk4l6B5qRPygImXqGzNSWiDISd
YeU/4XoZLXJBEP7/36r4mlnP2NWQ+c1ORjcsuDAZ8tDyhMvR4DVG95ESzjpTYv1wOmVB2lQrWnE
tygZIt60IlXitozo8uOekBnqWyDc1kuzZsYRfVNlwhCz7RsOq4zN8gkacl0fcquSNtBI29A+rc9L
Qeu6AcdPauWmbxtJV93H46pFptsR8zXo+Jln5m2P9QPZ3mvDkzldNTGLG+ukhN7IF2CCcagt/WoV
ZLq3qKC35WVcqeoSMEE/XeSrf3/mIJ1OyFQm+tsfhTceOFDXuUgl3E86bbR/I8Ur/bapwXpWpFxGI
pXLGaJXbzQGSTtyNEYrdENlh71I3OeYdw3xmzU2B3tbaWREOXtj2xjyW2tlv+vvHG6sloR1QklkG
MFtzs17W5U6ILetv

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer SERIAL NUMBER: *201803*

Issuer CN: *Citizen CA*

Issuer O: *Certipost N.V./S.A.*

Issuer L: *Brussels*

Issuer C: *BE*

Subject SERIAL NUMBER: *72020329970*

Subject GIVEN NAME: *Patrick Jean*

Subject SURNAME: *Kremer*

Subject CN: *Patrick Kremer (Signature)*

Subject C: *BE*

Valid from: *Sat Jun 02 00:04:19 CEST 2018*

Valid to: *Wed May 31 01:59:59 CEST 2028*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AF:B8:3B:56:B8:83:63:86:AC:DD:1E:0B:3C:E8:3B:B8:F1:F9:8A:71:F3:69:53:0E:C0:56:FF:F1:83:96:FB:D2:15:30:7
C:FF:57:97:49:03:37:93:2A:F8:4B:1B:94:B8:3E:4E:8A:77:61:3E:B7:5F:05:95:1A:27:A7:BD:06:BF:6F:A2:8E:D9:0F:93:B6:50:91:F7:B3:D3:27:2E:01:B2:D7:88:DC:76:4B:B7:DC:E4:61:BD:2C:62:5A:7C:32:60:06:04:D0:B9:
09:B5:68:35:4B:0D:0E:B9:DE:6A:91:E6:D0:0E:EA:01:1F:EA:FB:38:CD:11:12:2F:73:24:61:70:1f:AB:E4:BF:5A:87:04:68:6A:48:85:E3:55:00:5D:E2:3D:29:2F:11:ED:CB:BD:48:C5:FF:15:C7:58:5E:1A:32:FA:86:2B:A9:17:1
A:C7:9A:4D:C9:FD:86:04:DB:71:EB:96:D8:F0:22:12:BF:9E:0D:33:5C:CE:4C:06:04:31:57:C3:39:A7:18:53:CC:45:EC:F7:38:D9:3F:8C:82:A1:85:AF:13:CA:50:D2:7C:8F:CC:5F:73:83:B7:47:54:DE:3B:C9:10:A3:C8:7D:42:6
2:C4:13:DE:87:13:09:33:05:B1:4E:31:5B:36:EF:C2:2B:BB:49:F2:A4:F6:8B:54:B8:55:02:03:01:00:01

Authority Key Identifier *D9:34:21:3E:3A:42:25:6D:E1:BB:BF:BE:47:4C:F8:02:AD:E3:2F:54*

Authority Info Access

http://certs.eid.belgium.be/citizen201803.crt

http://ocsp.eid.belgium.be/2

Certificate Policies	*Policy OID: 2.16.56.12.1.1.2.1* *CPS pointer: http://repository.eid.belgium.be* *CPS text: [Gebruik onderworpen aan aansprakelijkheidsbeperkingen, zie CPS - Usage soumis à des limitations de responsabilité, voir CPS - Verwendung unterliegt Haftungsbeschränkungen, gemäss CPS]* *Policy OID: 0.4.0.194112.1.2*
CRL Distribution Points	*http://crl.eid.belgium.be/eidc201803.crl*
Extended Key Usage	*id_kp_emailProtection*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D2:06:4F:DD:70:F6:98:2D:CC:51:6B:86:D9:D5:C5:6A:EA:93:94:17:C6:24:B2:E4:78:C0:B2:9D:E5:4F:84:74*
TSL Type	*http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists*
Scheme Territory	*EU*
Mime Type	*application/vnd.etsi.tsl+xml*

Scheme Operator Name

Name	*[en]*	*European Commission*

Scheme Type Community Rules

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists*

List Issue Date Time

2021-10-26T01:00:00Z

Next Update

date Time	*2022-04-25T00:00:00Z*

Distribution Points

URI	*https://sede.minetur.gob.es/prestadores/tsl/tsl.xml*
URI	*https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf*

1 - TSP: Banco Santander, S.A.

.

TSP Name

Name	*[en]*	*Banco Santander, S.A.*
Name	*[es]*	*Banco Santander, S.A.*

TSP Trade Name

Name	*[en]*	*VATES-A39000013*
Name	*[en]*	*Santander*
Name	*[es]*	*Santander*
Name	*[en]*	*Banco Santander Central Hispano, S.A. CIF: A-39000013*
Name	*[en]*	*Banco Santander S.A. CIF: A-39000013*

PostalAddress

Street Address	*[es]*	*Ciudad Grupo Santander. Avd. de Cantabria s/n, edificio Pampa, planta 1*
Locality	*[es]*	*Boadilla del Monte*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28660*
Country Name	*[es]*	*ES*

PostalAddress

Street Address	*[en]*	*Ciudad Grupo Santander. Avd. de Cantabria s/n, edificio Pampa, planta 1*
Locality	*[en]*	*Boadilla del Monte*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28660*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.gruposantander.es*
URI	*[en]*	*mailto:certificacion.universitaria@gruposantander.com*

TSP Information URI

URI	*[en]*	*http://www.santander.com/csgs/Satellite/CFWCSancomQP01/es_ES/Corporativo/Sostenibilidad/Santander-Universidades/Otras-iniciativas.html?leng=en_GB*
URI	*[es]*	*http://www.gruposantander.es*

1.1 - Service (withdrawn): Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA*
Name	*[en]*	*Qualified Certificates issued by CA WG10 Qualified Identification Root CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *148047173988484494512973041456977244617*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIDwzCCAyygAwIBAgIQb2DZOwHrRP+mAnrmH5txyTANBgkqhkiG9w0BAQUFADCB0TEaMBgGA1UE
CBMRU2FudGFuZGVyIC0gU3BhaW4xHjAcBgNVBAcTFVBhc2VvIGRlIFBlcmVkYSwgOS0xMjE+MDwG
A1UEChM1QmFuY2ggU2FudGFuZGVyIENlbnRyYWwgSGlzcGFubywgUy5BLiBDSUY6IEEtMzkwMDAw
MTMxIzAhBgNVBAsTGkRpcmVjY2lvbiBkZSBVbmI2ZXJzaWRhZGVzMS4wLAYDVQQDEyVXRzEwIFF1
YWxpZmllZCBlZGVudGlmaWNhdGlvbiBSb290IENBMB4XDTA1MTEyNDAwMDAwMFoXDTE1MTEyMzIz
NTk1OVowgdExGjAYBgNVBAgTEVNhbnRhbmRlciAtIFNwYWluMR4wHAYDVQQHExVQYXNlbyBkZSBQ
ZXJlZGEsIDktMTIxPjA8BgNVBAoTNUJhbmNvIFNhbnRhbmRlciBDZW50cmFsIEhpc3Bhbm8sIFMu
QS4gQ0lGOiBBLTM5MDAwMDEzMSMwIQYDVQQLExpEaXJlY2Npb24gZGUgYW5pdmVyc2lkYWRlczEu
MCwGA1UEAxMlVGcxMCBRdWFsaWZpZWQgSWRlbnRpZmlpYXRpb24gU1m9vdCBDQTCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAtN/YPnb9/JTTvUQtLJjgGa8unu6OGT2Yhc30E82QhEuKeMA7VYxQ
uCiXJZ+uryO5JglDMexROH6Jn6irjUVBq9vJBncawtNtWY7pS2rOFhlG5flq9x07/K4HEBHagXtR
0PKMCRHVA4obZGWulZ36B/wWQjygKvOXK1ODA7t9N5kCAwEAAaOBmTCBljAPBgNVHRMECDAGAQH/
AgEAMAsGA1UdDwQEAwIBBjARBglghkgBhvhCAQEEBAMCAQYwIwYDVR0RBBwwGqQYMBYxFDASBgNV
BAMTC1ByaXZhdGUxLTMzMB0GA1UdDgQWBBQg/9bVbxm+4TSzCmZqtk+fdxEHbjABgNVHSMEGDAW
gBQg/9bVbxm+4TSzCmZqtk+fdxEHbjANBgkqhkiG9w0BAQUFAAOBgQAqwSBqibMfMXHInSexInDK
iRwWIYAI0DjQz5ZnF0v/vHbqOjNqpxyJHaO7z2xnHV5nQAIXYwDqk/ufjnBML/W3N6KV4z1VkDIY
RclaWTxXyltez1j7Qr1lCrt49lZr0uydjqsqE3eOBu6ByMWcCDL7T3HJRGkaD3GZGtdd6dPLbw==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *WG10 Qualified Identification Root CA*

Issuer OU: *Direccion de Universidades*

Issuer O: *Banco Santander Central Hispano, S.A. CIF: A-39000013*

Issuer L: *Paseo de Pereda, 9-12*

Issuer ST: *Santander - Spain*

Subject CN: *WG10 Qualified Identification Root CA*

Subject OU:	*Direccion de Universidades*
Subject O:	*Banco Santander Central Hispano, S.A. CIF: A-39000013*
Subject L:	*Paseo de Pereda, 9-12*
Subject ST:	*Santander - Spain*
Valid from:	*Thu Nov 24 01:00:00 CET 2005*
Valid to:	*Tue Nov 24 00:59:59 CET 2015*
Public Key:	*30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:B4:DF:D8:3E:76:FD:FC:94:D3:BD:44:2D:2C:98:E0:19:AF:2E:9E:EE:8E:19:3D:98:85:CD:F4:13:CD:90:84:4B:8A:78:C0:3B:55:8C:50:B8:28:97:25:9F:AE:AF:23:B9:26:09:43:31:EC:51:38:7E:89:9F:A8:AB:8D:45:41:AB:DB:C9:06:77:1A:C1:F3:6D:59:8E:E9:4B:6A:CE:16:19:46:E5:FB:6A:F7:1D:3B:FC:AE:07:10:11:DA:81:77:D1:D0:F2:8C:09:11:D5:03:8A:1B:64:65:AE:95:9D:FA:07:FC:16:42:3C:A0:2A:F3:97:2B:53:83:03:BB:7D:37:99:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Alternative Name	*CN=Private1-33*
Subject Key Identifier	*20:FF:D6:D5:6F:19:BE:E1:34:B3:0A:66:6A:B6:4F:9F:77:11:07:6E*
Authority Key Identifier	*20:FF:D6:D5:6F:19:BE:E1:34:B3:0A:66:6A:B6:4F:9F:77:11:07:6E*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1C:F1:AE:29:72:6D:13:08:73:8F:07:B6:80:8A:89:AB:29:C5:CC:BF:F8:C4:19:D3:5C:71:D9:68:AE:3D:1B:D1*

X509SubjectName

Subject CN:	*WG10 Qualified Identification Root CA*
Subject OU:	*Direccion de Universidades*
Subject O:	*Banco Santander Central Hispano, S.A. CIF: A-39000013*
Subject L:	*Paseo de Pereda, 9-12*
Subject ST:	*Santander - Spain*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

1.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

1.1.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA

Name [en] Qualified Certificates issued by CA WG10 Qualified Identification Root CA

Service digital identities

X509SubjectName

Subject CN: WG10 Qualified Identification Root CA

Subject OU: Direccion de Universidades

Subject O: Banco Santander Central Hispano, S.A. CIF: A-39000013

Subject L: Paseo de Pereda, 9-12

Subject ST: Santander - Spain

X509SKI

X509 SK I IP/W1W8ZvuE0swpmarZPn3cRB24=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased

Status Starting Time 2015-11-24T01:00:00Z

1.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA

Name [en] Qualified Certificates issued by CA WG10 Qualified Identification Root CA

Service digital identities

X509SubjectName

Subject CN:	*WG10 Qualified Identification Root CA*
Subject OU:	*Direccion de Universidades*
Subject O:	*Banco Santander Central Hispano, S.A. CIF: A-39000013*
Subject L:	*Paseo de Pereda, 9-12*
Subject ST:	*Santander - Spain*

X509SKI

X509 SK I	*IP/W1W8ZvuE0swpmarZPn3cRB24=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2009-04-13T00:00:00Z*

1.2 - Service (withdrawn): Santander Digital Signature

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Santander Digital Signature*
Name	*[es]*	*Santander Digital Signature*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*4828055370659501092*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGyjCCBLKgAwIBAgIIQwCyx4wTJCQwDQYJKoZIhvcNAQEFBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUJFIdG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1hcHJvZmVzaWNuYWwgQ0lGIEE2
MjYzNDA2ODAeFw0xMjA1MTYwOTIyNThaFw0zMDEyMzEwODM4MTVaMIGTMQswCQYDVQQGEwJFUzES
MBAGA1UECBMJU2FudGFuZGVyMR0wGwYDVQQHExRQYXNlbyBkZSBQZXJlZGEgOS0xMjEtMCsGA1UE
ChMkQmFuY2Rg U2FudGFuZGVyIFMuQS4gQ0lGOiBBLTM5MDAwMDEzMSQwIgYDVQQLDBtEaXJlY2Np
w7NuIGRlIFVuaXZlcnNpZGFkZXMxJDAiBgNVBAMTG1NhbnRhbmRlciBEaWdpdGFsIFNpZ25hdIHVy
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPKPxqLdb0p26KOq+JoQb1y8/Blqt6cl
gF6VoUT6nhn4P77Vuj54TkSmFyhnJhYpwhSmp+/IcFxlo7vfADjYdYCSi8+dpZhZA5bsG+KBOIa
XKKN2JsDsJVkipR5vl/dDZBrDJuFmDxxcLneU+RAwgeVDz+Gva7FTeEfwHt0xT5WlyYcBvIDbab
aCVkBLfNbylvNSW3i2QsTOT9hlrkstn0iFoXfp18d55CCAKfYfmLwQDNPsIzCRqLm7TsE5s0Sso
Y8cmN2aORYplj60uHfrHHyyel7lpZxoO6wr1fovKxraGLXMOYz2RxHrLD/HcJPb8F+VFSKbCcz
Ps2PrDMCAwEAAaOCAjkwggI1MEYGCCsGAQUFBwEBBDowODA2BggrBgEFBQcwAYYqaHR0cDovL3Nl
cnZpY2lvcy5maXJtYXByb2Zlc2lvbmFsLmNvbS9vY3NwMB0GA1UdDgQWBBRLjLqiLr71syS+ZtRN
Sl69Xf+/rTASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFGXN66s1HgA+fiV0wByc0c0cO
GmQvMIIBRwYDVR0gBIIBPjCCATowggE2BgorBgEEAcZ5CgoBMIIBIjAvBggrBgEFBQcCARYjaHR0
cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbS9jcHMwgflGCCsGAQUFBwICMIHllHoHiAEMAZQBy
AHQAaQBmAGkAYwBhAGQAbwAgAGQAZQAgAEEAdQB0AG8AcgBpAGQAYQBkACAAZABlACAAQwBlAHIA
dABpAGYAaQBjAGEAYwBpAPMAbgAuACAAQwBvAG4AcwB1AGwAdABlACAAbABhAHMAIABjAG8AbgBk
AGkAYwBpAG8AbgBlAHMAIABkAGUAIABlAHMAbwAgAGUAbgAgAGgAdAB0AHAAOgAvAC8AdwB3AHcA
LgBmAGkAcgBtAGEAcAByAG8AZgBlAHMAaQBvAG4AYQBsAC4AYwBvAG0ALwBjAHAAczA8BgNVHR8E
NTAzMDGgL6AthitodHRwczovL2NvbC5maXJtYXByb2Zlc2lvbmFsLmNvbS9mcHJvb3QuY3JsMA4G
A1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQUFAAOCAgEAm7OfvYv3SEjhUzl2tUiUzXaxUQm+bR2
oUFbbSv7UdIWc/xDzS0Iwo/UdFbVHDxgqg0QYdZjNjTTdHc+ThhRA0ooYG2LVSSlwPUn+SiyquKeJ
7bxgonzYMqnpbjRLJP91IOiq3b0XbhdZk4KBcObfpbtIiFejUux+8kKDUSlplHYVXfp10nxXEDlB
jDhsMq2ww AKekd07xSMdcjdazqfrFZcYGJI+O2DKLewpDb4mj+8VIS7SaD6iidnfm3uq2x0qrSxz
f1inunSs2W5eMnPH7ZsNX0uIPQWQ89zPUFJW6KZht7/kGE952fxOwOxyiOQzbqcmix1TWMp8I3Z
Y+zgYQbakoG0csdmWfMxSmCGnAFLMSWBYSVbWM6nLDdVyX0fIZgqKWorAa/NsoS+DAXRtF1PwBmj
FGrkmgDUjqFiO09uz5mPczcWQwmBXNxJamGuAG2mSGIYH9L0YLiwcuwGbPQWjoD6Z3mcIMQe
htMUPNCQKy6UK9Gc4M+Dlq7xUodSnvJAll/EZeQw7Mv++q1cFY+A4PD4unWq5mNiKiuDfG+dnTkl
uYxsUwcxIUwWr/Ict+IOhCGvz0YMRce6v1LcQKXFTG1wq6P1o7bvv9UeoJDG6biwzEGBBLa0PjE7
yhTJFFyciepScwQoTUb8DHMaxum51TQzr/Z/jUacfAaU=

-----END CERTIFICATE-----

Signature algorithm:

SHA1withRSA

Issuer CN:

Autoridad de Certificacion Firmaprofesional CIF A62634068

Issuer C:

ES

Subject CN:

Santander Digital Signature

Subject OU:

Dirección de Universidades

Subject O:

Banco Santander S.A. CIF: A-39000013

Subject L:

Paseo de Pereda 9-12

Subject ST:

Santander

Subject C:

ES

Valid from:

Wed May 16 11:22:58 CEST 2012

Valid to:

Tue Dec 31 09:38:15 CET 2030

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F2:8F:C6:A2:DD:6F:4A:76:E8:A3:AA:F8:9A:10:6F:5C:BC:FC:12:2A:B7:A7:25:80:5E:95:A1:44:FA:9E:19:F8:3F:BE
:D5:BA:3E:78:4E:44:A6:17:28:67:26:16:29:C2:14:A6:A7:EF:C8:70:5C:48:A3:BB:DF:00:38:D8:75:80:92:8B:CF:9D:A5:98:59:03:4E:5B:B0:6F:8A:04:E2:1A:5C:A2:8D:DA:52:6C:0E:C2:55:92:2A:51:E6:F9:7F:74:36:41:AC:
32:6E:16:60:F1:C5:C2:E7:79:4F:91:03:08:1E:54:3C:FE:1A:F6:BB:15:37:84:7F:01:ED:D3:14:F9:5A:5C:98:78:1B:C8:0D:B6:9B:68:25:64:04:B7:CD:6F:29:6F:35:25:B7:8B:64:2C:4C:E4:FD:86:5A:E4:B2:D9:F4:88:5A:17:7E:
9D:7C:77:9E:42:08:02:9F:61:FA:E6:2F:04:03:34:FB:08:CC:24:6A:2E:6E:D3:B0:4E:6C:D1:2C:E8:63:C7:26:37:66:8E:45:8A:65:8F:AD:1A:1C:57:47:7E:5B:72:C9:E2:3B:96:9D:B1:A0:EE:B0:AF:57:E8:BC:AC:6B:68:62:D7:
31:06:33:D9:1C:47:AC:B0:C9:1D:E2:4F:07:C1:7E:54:54:8A:6C:2C:F3:3E:CD:8F:AC:33:02:03:01:00:01

Authority Info Access

http://servicios.firmaprofesional.com/ocsp

Subject Key Identifier

4B:8C:BA:A2:2E:BE:F5:B3:24:BE:66:D4:4D:48:8E:BD:5D:FF:BF:AD

Basic Constraints

IsCA: true - Path length: 0

Authority Key Identifier

65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

Certificate Policies

Policy OID: 1.3.6.1.4.1.13177.10.10.1

CPS pointer: http://www.firmaprofesional.com/cps

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CRL Distribution Points

https://crl.firmaprofesional.com/fproot.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CB:C6:89:C8:7A:63:FA:73:23:A7:60:7C:C7:C4:57:B3:B4:50:57:2B:EF:A4:74:70:B6:1C:35:BF:07:9B:60:0B*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-10-22T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

1.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

1.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Santander Digital Signature*

Name *[es]* *Santander Digital Signature*

Service digital identities

X509SubjectName

Subject CN: *Santander Digital Signature*

Subject OU: *Dirección de Universidades*

Subject O: *Banco Santander S.A. CIF: A-39000013*

Subject L: *Paseo de Pereda 9-12*

Subject ST: *Santander*

Subject C: *ES*

X509SKI

X509 SK I *S4y6oi6+9bMkvmbUTUiOvV3/v60=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

1.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Santander Digital Signature*
Name	*[es]*	*Santander Digital Signature*

Service digital identities

X509SubjectName

Subject CN:	*Santander Digital Signature*
Subject OU:	*Dirección de Universidades*
Subject O:	*Banco Santander S.A. CIF: A-39000013*
Subject L:	*Paseo de Pereda 9-12*
Subject ST:	*Santander*
Subject C:	*ES*

X509SKI

X509 SK I	*S4y6oi6+9bMkvmbUTUiOvV3/v60=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2016-01-24T23:00:00Z*

1.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

2 - TSP: Dirección General de la Policía

.

TSP Name

Name	[en]	*Dirección General de la Policía*
Name	[es]	*Dirección General de la Policía*

TSP Trade Name

Name	[en]	*VATES-S2816015H*
Name	[en]	*Dirección General de la Policía*
Name	[es]	*Dirección General de la Policía*
Name	[en]	*DIRECCION GENERAL DE LA POLICIA*

PostalAddress

Street Address	[es]	*C/Miguel Ángel nº 5*
Locality	[es]	*Madrid*
State Or Province	[es]	*Madrid*
Postal Code	[es]	*28010*
Country Name	[es]	*ES*

PostalAddress

Street Address	[en]	*C/Miguel Ángel nº 5*
Locality	[en]	*Madrid*
State Or Province	[en]	*Madrid*
Postal Code	[en]	*28010*
Country Name	[en]	*ES*

ElectronicAddress

URI	[en]	*http://www.dnielectronico.es*
URI	[en]	*mailto:dnielectronico@dnielectronico.es*

TSP Information URI

URI	*[en]*	*http://www.dnielectronico.es/PDFs/practice_statement_certification_policy.pdf*
URI	*[es]*	*http://www.dnielectronico.es*

2.1 - Service (granted): Qualified Certificates issued by subordinated CA under the root CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by subordinated CA under the root CA*
Name	*[es]*	*Certificados Reconocidos emitido por CAs subordinadas de la CA Root*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *109308885283465423883312029610447405 9*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFvzCCA6egAwIBAgIQANKFcP2up9ZiEYQVxjG1yzANBgkqhkiG9w0BAQUFADBdMQswCQYDVQQG
EwJFUzEoMCYGA1UECgwfRElSRUNDSU9OIEdFTkVSQUwgREUgTEEgUE9MSUNJQTENMAsGA1UECwwE
RE5JRTEVMBMGA1UEAwwMQUMgUkFJWiBETkIFMB4XDTA2MDIxNjEwMzcyNVoXDTM2MDIwODIyNTk1
OVonXTELMAkGA1UEBhMCRVMxKDAmBgNVBAoMH0RJIk VDQ0lPYiBHRUSFUkFMERFIEsBIFBPYEID
SUExDTALBgNVBAsMBEROSUUxFTATBgNVBAMMDEFDIFJBSVogRE5JRTCCAiIwDQYJKoZIhvcNAQEB
BQADggIPADCCAgoCggIBAIAArQzDoyAHo2P/9zSgzc5qVAgXXbEBFafmuV+Kcf8Mwh3qN/Pek3/W
BU2EsIXXHAz0xJFwQA5ayJikgOgNM8AH87TrKE4csBmVCTNUswwKv1.DxKEsdr/BwL+C8ZvwaHoT
QMiXvBwIBwgKt5bvzCIU4OZlLeqyLrEJaRJOMNXY+LwAgC9Nkw/NLcbM7ufME7Epct5p/viNBi2
IJ4bn12ryTqtRWSzGM4REpxtHVFKlSeVZdN+cvni49YCdQS8g20jtDGV/FQ59wQfdqSLlkQDE
bHE0dNw56upPRGl/WNtYC1JxK+ypHVB0M/kpavr+mrTnzEVFbcpaJaIS487XOAU58BoJ9XZZzmJv
ejQNLNG8BBLsPVPI+tACy849lbXF4DkzZc85U8mbRvmdM/NZgAhBvm9LoPpKzqR2HIXir68U/nWWs
93+X5DNJpq++zis38S7BcwWcnGBMnTANI1SegWK75+Ay9xQHFKI3kenckZW004iQM0dvccMUafqm
LQEcG+rTLuUC9zP5yLw8UGjAZLlgND+qWKoVYgLNDTsSCEVqu/Wl16J9VGSEvprgBbZsQ3ZLvgQ
uML+UkUzmB04fNwVaTRzv6AsuxF7lM34Ny1vPc+DWsYem3RJj9nCjb4WdlDIWtElFvb2rlycWjCe
Zb7QmkiT1/poDXUxh/n3AgMBAAGjczB5MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEG
MB0GA1UdDgQWBBSORISfc8X/Lxsf2wFHY/BsDioG3ujA3BgNVHSAEMDAuMCwGBFUdIAAwJDAiBggr
BgEFBQcCARYWaHR0cDovL3d3dy5kbmlILmVzL2RwYzANBgkqhkiG9w0BAQUFAAOCAgEAdeVzyVFR
L4sZoIfp/642Nqb8QR/jHtdxYBnGb5oCML1ica1z/pEiTuQmQESpmgmIzFp3JpzlhJ5JUQvg78Gf
Q+9xnO5Bt8VQHzKEmKG8fcfj9mtK07alyiXu5aaGvix2XoE81SZEhmWFYBnOf8CX3r8VUQWua5
ov+4qGIeFM3ZP76jZUjFO9c3zg36KJDav/njUUclfUrTZ02HqmK8Xux6gERR9958KvWXlMryEWbW
Un/kOnB1BM0779QZvdRVr809dJB4bTaqEP+axJIEzRdrvJCowIIyaMdbBOXapT7qFvdeWSobEz
xNdq/fgOym6C2ee7WSNOtfkRHS9rU/V7ESDqQRKQMkbbMTupwVtzaDpGG4z+l7dWuWGZzE7wg/o3
8d4cnRxxwOTw8Rzgi6omB1kopqM91QITc/qgcv1WwmZY691jJb4eTXV3OtBgXk4hF5v8W9iduR
zlqFYDkdW+lqL0Ml28I6JNMVsKLxjKB9a0gJE/+iTGaK7HBSCVOMMMy41bok3DCZPqFet9+BrOw3
vk6bJ1ejGzbVH8Gtz/kMlD95uC7qMJaGBrÚY2Y96IFxOJScPt9a9NrHTCbt7Uhnjt8SAnNhENqY
Mahgy34Hp9C3BUOJW82FJtmwUa/3jFKqEqdY35KbZ/Kd8ub0aTH0FufedJse3ZoFAa0=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *AC RAIZ DNIE*

Issuer OU: *DNIE*

Issuer O: *DIRECCION GENERAL DE LA POLICIA*

Issuer C: *ES*

Subject CN: *AC RAIZ DNIE*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

Valid from: *Thu Feb 16 11:37:25 CET 2006*

Valid to: *Fri Feb 08 23:59:59 CET 2036*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:80:00:AD:0C:C3:A3:20:07:A3:63:FF:F7:34:A0:CD:EE:6A:54:08:17:5D:B1:01:15:A7:E6:B9:5F:8A:71:FF:0C:C2:1D:
EA:37:F3:DE:93:7F:D6:05:4D:84:B2:D5:D7:1C:0C:F4:C4:91:70:40:0E:5A:C8:98:A4:80:E8:0D:33:C0:07:F3:B7:F5:AC:A1:38:7A:C0:66:54:24:FC:52:CC:30:2A:F2:C3:C4:A1:2C:76:BF:C1:C0:BF:82:F1:9B:F0:68:7A:13:40:
C8:97:BC:1C:25:07:08:0A:B7:96:EF:CC:29:54:E0:E6:65:2D:EA:B2:2E:B1:09:69:12:4E:30:D5:D8:F8:BC:00:80:2F:4D:93:0F:CD:2E:57:1B:33:BB:9F:30:4E:C4:A5:CB:79:A7:FB:E2:34:18:B6:20:9E:1B:9F:5D:A7:C9:3A:AD
:45:64:B3:18:CE:11:12:9C:6D:1E:55:45:28:84:9C:57:67:4D:F9:CB:E2:8B:8F:58:09:D4:39:FF:C8:36:D2:38:E2:0C:65:7F:15:0E:7D:C1:07:DD:A9:22:DF:91:00:C4:6C:71:34:74:DC:39:EA:EA:4F:44:69:7F:58:DB:58:0A:52:71
:2B:EC:A9:1D:50:74:33:F9:29:6A:FA:FE:99:F4:E7:CC:45:45:6D:CA:5A:25:A2:12:E3:CE:D7:38:05:39:F0:1A:09:F5:76:59:CE:62:6F:7A:34:0D:2C:D1:BC:04:12:EC:3D:53:C8:FA:D0:02:CB:CE:3D:21:B5:C5:E0:39:33:65:C
F:39:53:C9:9B:46:F9:9D:33:F3:59:80:08:41:BE:6F:4B:A0:FA:4A:CE:A4:76:1C:85:E2:AF:AF:14:9D:65:AC:F7:7F:97:E4:33:49:A6:AF:BE:CE:2B:37:F1:2E:C1:73:05:9C:9C:60:4C:9D:30:0D:97:54:9E:81:62:BB:E7:E0:2F:F7
:14:07:14:A9:77:91:E9:DC:91:95:8E:D3:88:90:33:47:6F:71:C3:14:69:FA:A6:2D:01:1E:1B:EA:D3:2E:E2:7F:0B:DC:CF:E7:22:F0:F1:41:A3:01:92:E5:80:D3:BE:A9:62:A8:55:88:0B:34:34:EC:DC:21:15:AA:EF:D6:22:5E:89:F
5:51:92:13:2A:6F:80:16:D9:B1:0D:D9:2E:F8:10:B8:C2:FE:52:45:33:9C:1D:38:7C:DC:15:69:34:73:BF:A0:2C:BB:11:7B:94:CD:F8:37:2D:6F:3D:EF:83:5A:C6:1E:9B:74:49:8F:D9:C2:8D:BE:16:76:50:C8:5A:D1:25:16:F6:F6:
CC:8C:9C:5A:30:9E:65:BE:D0:9A:48:93:D7:FA:68:0D:75:31:87:F9:F7:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *8E:45:F4:9F:73:C5:FF:2F:1B:05:DB:01:47:60:1B:03:8A:81:B7:BA*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.dnie.es/dpc

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *73:97:10:C5:24:5E:33:EC:8A:24:3A:1B:20:04:8F:C9:D5:F4:52:85:99:21:38:45:C1:64:D0:04:B8:B6:67:F9*

Certificate fields details

Version: *3*

Serial Number: *102366917162036235385844356259614709 2*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFvzCCA6egAwIBAgIQAMUmyW4QlO1DT/e1+2eflDANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQG
EwJFUzEoMCYGA1UECgwfRE1FSRUNDSU9OIEdlFTkVSQUwgRE1lgTEEgUE9MSUNJQTEnMAsGA1UECwwE
RE5JRTEVMBMGA1UEAwwMQUMgUkFJWiBETklFMB4XDTA2MDIxNjEwMzcyNVoXDTM2MDIwODIyNTk1
OVowXTELMAkGA1UEBhMCRVMxKDAmBgNVBAoMH0RJUkVDQ0lPTiBHRU5FUkFMIERFIExBIFBPTElD
SUExDTALBgNVBAsMBEROSUUxFTATBgNVBAMMDEFDIFJBSVogRE5JRTCCAiIwDQYJKoZIhvcNAQEB
BQADggIPADCCAgoCggIBAIAArQzDoyAHo2P/9zSgzc5qVAgXXbtEBFafmuV+Kcf8Mwh3qN/Pek3/W
BU2IstXXIAz0xIFwQA5ayJdgQgNMbAH87TrKE4esBmVCT9UsswvKvLDxKEsdr/BwL+CXZvwaHoT
QMiXvBwlBwgKt5bvzC1U4OZlLcqyLrEJaRJOMNXY+LwAgC9Nkw/NLlcbM7uIME7Epct5p/viNBi2
I4bn12nyTqtRWSzGM4REpxtHIVFKIScV2dN+cvvi49YCdQS/8g20jjiDGV/FQS9wQ0dqSLfkQDE
bHE0dNw56upPRGl/WNtYC1IxK+ypHVB0M/kpavr+mTnzEVFbcpaIaIS487XOAU58Bo J9XZZzmJv
cjQNLNG8BBLsPVPf+tACy849lbXF4DkczZc85U8mbRvmdM/NZgAbBvm9LoPpKcqR2HIXzr6lUnWWs
93+X5DNJpq++zis38S7BcwWcnGBMnTANl1SegWK75+Av9xQHFKI3kenckZWO04iQM0dvccMUafqm
LQEcG+rTLuJ/C9zP5yLw8UGjAZLlgNO+qWKoVYgLNDTs3CEVqu/Wlf6J9VGSEypvgBbZsQ3ZLvgQ
uML+UkUzmB04fNwVaTRzv6AsuxF7lM34Ny1vPe+DWsYem3RJj9nCjb4WdlDIWtEIFvb2zlycWjCe
Zb7QmktT1poDXUxb/n3AgMBAAGjezB5MA8GA1UdEwEBwQFMAMBAf8wDgYDVR0PAQH/BAQDAgEG
MB0GA1UdDgQWBBSORfSfc8X/LxsF2wFHYBsDioG3ujA3BgNVHSAEMDAuMCwGBFUdIAAwJDAtBggr
BgEFBQcCARYWaHR0cDovL3d3dy5kbmllLmVzL2RwYzANBgkqhkiG9w0BAQsFAAOCAgEAF/n5Mo3T
NqhTHhYEm8Wbdh8NmPrU4owmsjL7T4Ot0fRHuRSS/48lYaK7/krIGFVyZ1AqMSCWjcw3O+G3QxF7
bSkTsZkEG/wgnzU9pD1TW66/v5UNxMWyiLOVRt19bC3qDb9gua3vcqLJINXL YKOh0YR44bYjfp
gXGWSkmk3K9aXOcbBxPHUq7IbtK0Vdq5SloNxYNw2awdfF9J0s91pOtOOl/XTRz/EE6BEYYwBaNA
4lsTfMFNKdor0VwsN418i08ba8gEKMQ29CqHyCB4VzLf1QHvL6rVQ8tNTkOgt/ozx1Xo0zzJY6J
DgaQ2Rzdk6xrVNi1/SN9vNn1WTIAK8BreQMfYh+vBYYVEXuXU/8Wx7lLn4H7s8Jy5EUdNvznjkB
P5qmrHSLl61eM1/b3rxCS1sgUF7n9KmuBWk0tu+4v1i0V/O2YdEgpTwNDR+Utr+JoikLNgF09k8F
jfQ45iNj7VM0AsbJSicpVmhhi58Re7m3yrObjMg0VDzMQM2hFYh9uRUV0lQ8lL0qVFK8VodNYxh
FWT+syvMuxkb520jFCbaUAbIuEt0qbaORyNhcTWWObK29dg1fHvFGR2r8ZE09/ceeVKgcvyYfoe+Q
Bx3200AGbMrhFN1E30kORua2628QZv5yKZL45hMDN4MvTN3QnzB5XillEH4avjfG9Q=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *AC RAIZ DNIE*

Issuer OU: *DNIE*

Issuer O: *DIRECCION GENERAL DE LA POLICIA*

Issuer C: *ES*

Subject CN:	*AC RAIZ DNIE*
Subject OU:	*DNIE*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*
Valid from:	*Thu Feb 16 11:37:25 CET 2006*
Valid to:	*Fri Feb 08 23:59:59 CET 2036*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:80:00:AD:0C:C3:A3:20:07:A3:63:FF:F7:34:A0:CD:EE:6A:54:08:17:5D:B1:01:15:A7:E6:B9:5F:8A:71:FF:0C:C2:1D:EA:37:F3:DE:93:7F:D6:05:4D:84:B2:D5:D7:1C:0C:F4:C4:91:70:40:0E:5A:C8:98:A4:80:E8:0D:33:C0:07:F3:B7:F5:AC:A1:38:7A:C0:66:54:24:FC:52:CC:30:2A:F2:C3:C4:A1:2C:76:BF:C1:C0:BF:82:F1:9B:F0:68:7A:13:40:C8:97:BC:1C:25:07:08:0A:B7:96:EF:CC:29:54:E0:E6:65:2D:EA:B2:2E:B1:09:69:12:4E:30:D5:D8:F8:BC:00:80:2F:4D:93:0F:CD:2E:57:1B:33:BB:9F:30:4E:C4:A5:CB:79:A7:FB:E2:34:18:B6:20:9E:1B:9F:5D:A7:C9:3A:AD:45:64:B3:18:CE:11:12:9C:6D:1E:55:45:28:84:9C:57:67:4D:F9:CB:E2:8B:8F:58:09:D4:39:FF:C8:36:D2:38:E2:0C:65:7F:15:0E:7D:C1:07:DD:A9:22:DF:91:00:C4:6C:71:34:74:DC:39:EA:EA:4F:44:69:7F:58:DB:58:0A:52:71:2B:EC:A9:1D:50:74:33:F9:29:6A:FA:FE:99:F4:E7:CC:45:45:6D:CA:5A:25:A2:12:E3:CE:D7:38:05:39:F0:1A:09:F5:76:59:CE:62:6F:7A:34:0D:2C:D1:BC:04:12:EC:3D:53:C8:FA:D0:02:CB:CE:3D:21:B5:C5:E0:39:33:65:CF:39:53:C9:9B:46:F9:9D:33:F3:59:80:08:41:BE:6F:4B:A0:FA:4A:CE:A4:76:1C:85:E2:AF:AF:14:9D:65:AC:F7:7F:97:E4:33:49:A6:AF:BE:CE:2B:37:F1:2E:C1:73:05:9C:9C:60:4C:9D:30:0D:97:54:9E:81:62:BB:E7:E0:2F:F7:14:07:14:A9:77:91:E9:DC:91:95:8E:D3:88:90:33:47:6F:71:C3:14:69:FA:A6:2D:01:1E:1B:EA:D3:2E:E2:7F:0B:DC:CF:E7:22:F0:F1:41:A3:01:92:E5:80:D3:BE:A9:62:A8:55:88:0B:34:34:EC:DC:21:15:AA:EF:D6:22:5E:89:F5:51:92:13:2A:6F:80:16:D9:B1:0D:D9:2E:F8:10:B8:C2:FE:52:45:33:9C:1D:38:7C:DC:15:69:34:73:BF:A0:2C:BB:11:7B:94:CD:F8:37:2D:6F:3D:EF:83:5A:C6:1E:9B:74:49:8F:D9:C2:8D:BE:16:76:50:C8:5A:D1:25:16:F6:F6:CC:8C:9C:5A:30:9E:65:BE:D0:9A:48:93:D7:FA:68:0D:75:31:87:F9:F7:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*8E:45:F4:9F:73:C5:FF:2F:1B:05:DB:01:47:60:1B:03:8A:81:B7:BA*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.dnie.es/dpc*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F5:79:21:10:81:7A:86:D4:FE:24:4A:C2:A8:B1:0B:5B:0B:F4:CE:86:26:66:1A:B9:84:47:0A:87:87:98:30:F5*

X509SubjectName

Subject CN:	*AC RAIZ DNIE*
Subject OU:	*DNIE*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.crt*
URI	*[es]*	*https://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.crt*

URI	*[en]*	*https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt*
URI	*[es]*	*https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt*
URI	*[en]*	*https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt*
URI	*[es]*	*https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt*
URI	*[en]*	*http://www.dnielectronico.es/PDFs/Politicas_de_Certificacion_v2.1.pdf*
URI	*[es]*	*http://www.dnielectronico.es/PDFs/Politicas_de_Certificacion_v2.1.pdf*
URI	*[en]*	*https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt*
URI	*[es]*	*https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt*
URI	*[en]*	*https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt*
URI	*[es]*	*https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt*
URI	*[en]*	*https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt*
URI	*[es]*	*https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt*

2.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.2.2.2.11*

Description

2.1.4 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by subordinated CA under the root CA*
Name	*[es]*	*Certificados Reconocidos emitido por CAs subordinadas de la CA Root*

Service digital identities

X509SubjectName

Subject CN:	*AC RAIZ DNIE*
Subject OU:	*DNIE*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*

X509SKI

X509 SK I	*jkX0n3PF/y8bBdsBR2AbA4qBt7o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2006-12-11T00:00:00Z*

2.1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.2 - Service (granted): Qualified Certificates issued by subordinated CA under the root CA for Public Administration

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by subordinated CA under the root CA for Public Administration*

Name *[es]* *Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *97711293539174917544610076615930313 4*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFvjCCA6agAwIBAgIQALwvYx2O1YN6UxQOi3BxjANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQG
EwJFUzEoMCYGA1UECgwIREISRUNDSU9OIEdFTkVSQUwgRE1gTEEgUE9MSUNQTEMMAoGA1UECwwD
Q05QMRQwEgYDVQQDDAtBQyBSQUlalERHUDAeFw0wNzAxMjUxMjA1MDhaFw0zNzAxMjUxMjA1MDha
MFsxCzAJBgNVBAYTAkVTMSgwJgYDVQQKDB9ESVJFQ0NJT04gR0VORVJBTCBERSBMQSBQT0xJQ0lB
MQwwCgYDVQQLDANDT1AxFDASBgNVBAMMC0FDIFJBSVogREdQMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAgBD1t16oMJxvuxuIDly6gfgzPmmDMFvPvqi0AOcjyxu6773KthVjpMatQ
qiGae3Yj83upv7YFygaj/U02EeEIeQQEf+QJ+B+LX+oGLPbU5g8/W1eFcnXC4Jg2inP7L2qcEfA1
80AsT1UqmHTc7kRI3N6yJZZiHkM4hpjI3vgsCxUQtXw+XAZYtaRbjFO69tTSdhpbXN4fvOQwHNlc
nF1GMxsih7tgGUwRIY2EVfh7EGYvXt2mpHiEIeSp1s2WBxzgiWU1IufiDo18olZj859o4HkNBD0s
x6LVPPbm/iNuMIM6aIRwc72SAMgZmIyNDOHZIgExL8DNUiTzXYzqr7RX+kn59RYLwIEimIRQLkK
xyYlZeFbuI5Io7Uz3vKANcTbUuCymA0+ZA9ESlrz8kA6HV0+fMePUBYnocUO5fFXjxtScOqrQ
t+K+gGm4TubalBoL7ECGzs3CmKtnuyOH+KFO/8q71Fxhn3WqlKgO7dBUhp0U/7dr4R2bF4ry1Nnq
ZWObCuBHKqyL80Dx+6zaGsTo7UBLNdcA4sXAzIoAMUqHb/77rqu45dWJlhQA5V3qolwowwuTdZwC
1ec2AWwA6gM2uchNJsPWWmQrkXvkhu2rf756cKwgR7y22517q/B9MNx7lnsZbMbOWUwQuei3Uco
IgCFs2TWCbhxHNkCAwEAAaN+MHwwDwYDVR0TAQH/BAUwAwEB zAOBgNVHQ8BAf8EBAMCAQYwHQYD
VR0OBBYEFA6cduGiLokzQfLjPmxbFkW9vYaOMDoGA1UdIAQzMDEwLwYEVR0gADAnMCUGCCsGAQUF
BwIBFhlodHRwOi8vd3d3LnBvbGljaWEuZXMvZHBjMA0GCSqGSIb3DQEBBQUAA4ICAQBslvw3pwCj
21vCctyL7YOmnINjJFp4TNFfNnDwSsuonqOjwppXCEFJ6MkOeCUOy9vXznNoYtoDd/tXAn++997
Sd7PB9vXnu7ErHKx+c74obKpqIBoVv9fwPpl0bO3YPrTq9EGPLM8mbc1IEivPlL2mQ7k7Bz2p8gp
ytcCZRe08Jd5m+AeYPrHUDeF6ZllnH7SIrtP3Bp8zwnNIFbNtkyrCyWtN8Ajo3RXqecM/bs+YgGz
jVbDToQUBkBC uoG3XU+QYSQ79yZsvjTCsFKBYnXXijiGZSokx33iauYOPIyaNu/ulMloSNUwWZ5W
BPqJXWlkZ+deApxZLXJLFMSTjFeFdpZUgOC1wrRkxXidWQwr4566fYWhYH0w+hwK9gD6NEsMA3D7
NOPCTCOx9Qst5848Rs/VJ4F+ZFm14jyTYLygIkNieB+tSXVyC9Lg+Tvay85VycZMSZ3PpCmpNzaQ
xVZl9XCfs8R6Ew4pG91eOA0BjsI1ZHY7Hl9e5Pomup/jTA6JwlCYooEiBM31Gdwe/3oUFNzB+NvOW
dwb+ZG6va70j98EdipGWoLvjv/oJlFN2q1Nrt/u7whKp+VsVOjuZMrSpw9C+Ec4yiL ha5RRiXnHX
1cqwT694KIDQZIgqQChQDeDqrvCphtdHdxFQ5NBzt2HKhaSh8ggDdOdpH451rB45Jg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *AC RAIZ DGP*

Issuer OU: *CNP*

Issuer O: *DIRECCION GENERAL DE LA POLICIA*

Issuer C: *ES*

Subject CN: *AC RAIZ DGP*

Subject OU: *CNP*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

Valid from: *Thu Jan 25 13:05:08 CET 2007*

Valid to: *Sun Jan 25 13:05:08 CET 2037*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:80:10:F5:B7:5E:B3:30:9C:6F:A3:1B:88:0E:5C:AD:EA:97:E0:CC:F9:A6:7C:93:05:BC:FC:A8:8F:40:0E:C6:3C:B1:BB
:A7:FB:EC:AF:ED:85:5F:E9:31:AB:50:AA:31:9A:7B:76:23:F3:7B:A9:BF:B6:05:CA:0A:BF:8D:4D:36:11:E1:08:79:04:04:7F:E4:09:F8:1F:8B:5F:EA:06:2C:F6:D4:E6:0F:3F:5B:57:85:72:75:C2:E0:98:36:8A:93:FB:2F:6A:9C:
11:F0:35:F3:40:2C:4F:55:2A:98:74:DC:EE:44:48:DC:DE:B2:25:96:62:1E:43:38:86:98:DF:DE:F8:2C:0B:15:10:B5:7C:3E:5C:06:58:B5:A4:5B:8C:53:BA:F6:D4:D2:75:BA:5B:5C:DE:1F:BC:E4:30:1C:D9:5E:9C:5D:46:33:1B:
22:87:BB:60:19:4C:11:95:8D:84:55:F8:7B:10:66:2F:5E:DD:A6:B6:91:E2:10:87:92:A7:5B:36:58:1C:73:82:25:94:D4:8B:9F:88:3A:35:F2:89:59:8F:CE:7D:A0:79:0D:04:3D:2C:C7:A2:D5:3C:FB:A7:FE:C2:0D:B8:CD:4C:E9:A
0:51:C1:CE:F6:E5:C3:20:66:62:32:34:33:87:66:4A:84:C4:BF:03:35:48:93:CD:76:33:AA:BE:D1:FD:7F:A4:9F:9F:51:60:BC:08:12:67:D1:40:B9:0A:C7:26:25:65:E1:5B:B8:E2:39:9F:B5:33:DE:F2:80:35:C4:DB:52:E0:B2:98:0
D:3E:64:0F:44:4A:5A:F3:F2:40:3A:7C:75:74:F9:F3:1E:3D:40:58:9E:87:22:24:EE:5F:15:7F:E3:C6:D4:9C:3A:AA:D0:B7:E2:BE:80:69:B8:4E:E6:DA:94:1A:0B:EC:40:86:CE:CD:C2:98:AB:67:BB:23:87:F8:A1:4E:FF:CA:BB:
D4:5C:61:9F:75:AA:94:A8:0E:ED:D0:54:86:9D:08:FF:B7:6B:E1:1D:9B:17:8A:F2:D4:D9:EA:65:63:9B:0A:E0:5F:2A:AC:8B:F3:40:F1:FB:AC:DA:1A:C4:E8:ED:40:4B:35:D7:00:E2:C5:C0:AC:9A:00:31:4A:87:6F:FE:FB:A
E:AB:B8:E5:D5:89:22:14:00:E5:5D:EA:A2:5C:28:C3:0B:93:75:9C:02:D5:E7:36:01:6C:00:EA:03:1F:DA:E7:21:34:9B:0F:59:69:90:AE:45:EF:92:1B:B6:AC:8E:F9:E9:C2:B0:81:1E:F2:DB:6E:75:EE:AF:C1:F4:C3:71:EC:89:E
C:65:B3:1B:39:65:30:42:E7:A2:DD:47:28:22:00:85:B3:64:D6:09:B8:71:1C:D9:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier

0E:9C:76:E1:A2:2E:89:33:41:F2:E3:3E:6C:5B:16:45:BD:BD:86:8E

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.policia.es/dpc

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

97:E9:F2:C6:2C:95:F1:F0:FF:B0:A6:DF:29:C4:E7:64:7E:C9:06:FB:62:D3:62:26:FD:81:1D:41:22:74:6C:89

Certificate fields details

Version:

3

Serial Number:

100975973575478694020384208965744905 4

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFvjCCA6agAwIBAgIQAMJ4/6rRByxyp40tJL46XjANBgkqhkiG9w0BAQsFADBbMQswCQYDVQQG
EwJFUzEoMCYGA1UECgwfRElSRUNDSU9OIEdFTkVSQUwgREUgTEEgUE9MSUNJQTEMMAoGA1UECwwD
Q05QMRQwEgYDVQQDDAtBQyBSQUlaERHUDAeFw0wNzAxMjUxMjA1MDhaFw0zNzAxMjUxMjA1MDha
MFsxCzAJBgNVBAYTAkVTMSgwJgYDVQQKDB9ESVJFQ0lOIFQ0NJT04gR0VORVJBTCBERSBMQSBQT0xJQ0lB
MQwwCgYDVQQLDANDTIAxEDASBgNVBAMMC0FDIEJBSVogREdQMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAgBD1t116zMJxvoxulDlyt6pfgzPmmDMFvPyoj0AOxjyxu6i77K/thV/pMatQ
qjGae3Yj83upv7YFygq/jU02EcEIcQQEF+QJ+B+LX+oGLPbU5g8/W1eFcnXC4Jg2jnP7L2qcEfA1
80As1TiUqmHTc7kRI3N6yJZZtHkM4hnjt3vgsCxUQtXw+XAZYtaRbjFO69rTSdhpbXN4tvOQwHNle
nFIGMxsih7tgGUwRfY2EVtb7EGYvXi2mtpHEIcSpIs2WBxzgiWU1Iu6Dn18ol2j859ot4IkNBD0ts
x6LVPPun/slNuM1M6aBRwc725cMgZmlyNDOHZkqExL8DNUiTzXYxqr7R/X+kn59RYLwIEmfRQLkK
xyYIZeFbuOI5n7Uz3vKANcTbUuCymA0+ZA9ESlrz8kA6fHV0+fMePUBYnocuJO5fFX/jxtScOqrQ
t+K+gGm4TubalBoL7ECGzs3CmKmuyOH+KFO/8q71Fxhn3WqlKgO7dBUhp0I/7dr4R2bF4ry1Nnq
ZWObCuBtKqyL80Dx+6zatGsTo7UBLNdcA4sXAzIoAMUqtHb/77tqu45dWVlbQA5V3qohwowwuTdZwC
1ec2AWwA6gM2uchNJsPWWmQrkXvkhu2rt756cKwgR7y22517q/B9MNx7lnsZbMbOWUwQuei3Uco
IgCFs2TWCBhxHNkCAwEAAaN+MHwwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAI8EBAMCAQYwHQYD
VR0OBBYEFA6cduGiLokzQtLjPmxbFkW9vYaOMDoGA1UdIAQzMDEwLwYEVR0gADAnMCUGCCsGAQUF
BwIBFhlodHRtcOi8vdSd3L nBvbGljaWEuZXMvZHBjMA0GCSqGSIb3DQEBCwUAA4ICAQATTA4j4gS8
tOVJZu0OgYt05dniekIY6G3xLpbalQtKPPPwN7UpSkBIoN1IeFVrlY+PwAThYGi3xgC4XCjQVnr5
1nLgeOGlYCeF0plqMeT4qETd8k8JX4Y8gn9T31O2/0D87qM5K2FR8Kxnc9lCPRPntjwvaM2g6Xgt
/uY1VTa/+ODWutEd4zcGUixxP9fQWk/qkAqVaqyz8aUVWw9GRC9eoroMfpzZWtE1S5vf6VBkIaHD
zURmCrh5uZ79SLdUKDfe6B7Iw75QhuRPpn4+DbvZTBqbHQ2VKpn5L2dfBoAxFeBOXczRIMbIdEYxY6
agXDPPshgKkWmv3sxu7BzF74lG8VQPFp7TtZSEZ8G5hL4RG2LqzAcK6ahjxkbqJPsRUq15bs0itow
dTo4YCA1Syn6eYu3gq2PDLFK3q48zCjvwk3rACoM1yw7BFUN4l70vORqLmefYpzm2b6HH4mKTpwl
icFdL24vYVShAwRXaJYUcw2rFhTgms2uqpkPQNxR8PA7/3oB5sTZh6DEdWX80XCLA/3bdY+b70SV
SMGcSEPTFGv2AIIu9zIGY7kpe7ngHVy9dWkf9j9MhBz2gG0ZX8j6yrI4sk QHVWFy4SotbavOv6SJ
nUc2fjitRPvirqCZSQ1OICByZY/hZ3asYgwv2mBlS47dfj6aEapRz07LvPZIAo9MQ==

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer CN:

AC RAIZ DGP

Issuer OU:

CNP

Issuer O:

DIRECCION GENERAL DE LA POLICIA

Issuer C:

ES

Subject CN:

AC RAIZ DGP

Subject OU:

CNP

Subject O:

DIRECCION GENERAL DE LA POLICIA

Subject C:

ES

Valid from:

Thu Jan 25 13:05:08 CET 2007

Valid to:

Sun Jan 25 13:05:08 CET 2037

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:80:10:F5:B7:5E:B3:30:9C:6F:A3:1B:88:0E:5C:AD:EA:97:E0:CC:F9:A6:7C:93:05:BC:FC:A8:8F:40:0E:C6:3C:B1:BB:A7:FB:EC:AF:ED:85:5F:E9:31:AB:50:AA:31:9A:7B:76:23:F3:7B:A9:BF:B6:05:CA:0A:BF:8D:4D:36:11:E1:08:79:04:04:7F:E4:09:F8:1F:8B:5F:EA:06:2C:F6:D4:E6:0F:3F:5B:57:85:72:75:C2:E0:98:36:8A:93:FB:2F:6A:9C:11:F0:35:F3:40:2C:4F:55:2A:98:74:DC:EE:44:48:DC:DE:B2:25:96:62:1E:43:38:86:98:DF:DE:F8:2C:0B:15:10:B5:7C:3E:5C:06:58:B5:A4:5B:8C:53:BA:F6:D4:D2:75:BA:5B:5C:DE:1F:BC:E4:30:1C:D9:5E:9C:5D:46:33:1B:22:87:BB:60:19:4C:11:95:8D:84:55:F8:7B:10:66:2F:5E:DD:A6:B6:91:E2:10:87:92:A7:5B:36:58:1C:73:82:25:94:D4:8B:9F:88:3A:35:F2:89:59:8F:CE:7D:A0:79:0D:04:3D:2C:C7:A2:D5:3C:FB:A7:FE:C2:0D:B8:CD:4C:E9:A0:51:C1:CE:F6:E5:C3:20:66:62:32:34:33:87:66:4A:84:C4:BF:03:35:48:93:CD:76:33:AA:BE:D1:FD:7F:A4:9F:9F:51:60:BC:08:12:67:D1:40:B9:0A:C7:26:25:65:E1:5B:B8:E2:39:9F:B5:33:DE:F2:80:35:C4:DB:52:E0:B2:98:0D:3E:64:0F:44:4A:5A:F3:F2:40:3A:7C:75:74:F9:F3:1E:3D:40:58:9E:87:22:24:EE:5F:15:7F:E3:C6:D4:9C:3A:AA:D0:B7:E2:BE:80:69:B8:4E:E6:DA:94:1A:0B:EC:40:86:CE:CD:C2:98:AB:67:BB:23:87:F8:A1:4E:FF:CA:BB:D4:5C:61:9F:75:AA:94:A8:0E:ED:D0:54:86:9D:08:FF:B7:6B:E1:1D:9B:17:8A:F2:D4:D9:EA:65:63:9B:0A:E0:5F:2A:AC:8B:F3:40:F1:FB:AC:DA:1A:C4:E8:ED:40:4B:35:D7:00:E2:C5:C0:AC:9A:00:31:4A:87:6F:FE:FB:AE:AB:B8:E5:D5:89:22:14:00:E5:5D:EA:A2:5C:28:C3:0B:93:75:9C:02:D5:E7:36:01:6C:00:EA:03:1F:DA:E7:21:34:9B:0F:59:69:90:AE:45:EF:92:1B:B6:AC:8E:F9:E9:C2:B0:81:1E:F2:DB:6E:75:EE:AF:C1:F4:C3:71:EC:89:EC:65:B3:1B:39:65:30:42:E7:A2:DD:47:28:22:00:85:B3:64:D6:09:B8:71:1C:D9:02:03:01:00:01

Basic Constraints

IsCA: true

Subject Key Identifier

0E:9C:76:E1:A2:2E:89:33:41:F2:E3:3E:6C:5B:16:45:BD:BD:86:8E

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.policia.es/dpc

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

1F:30:4D:5D:DA:90:47:60:C4:B8:D6:2F:14:F5:19:62:A7:06:CD:C0:2C:5B:70:F1:50:33:A0:4F:CD:36:45:B8

X509SubjectName

Subject CN:

AC RAIZ DGP

Subject OU:

CNP

Subject O:

DIRECCION GENERAL DE LA POLICIA

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-07-16T00:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.policia.es/DPC/dpc.pdf*

URI *[es]* *http://www.policia.es/DPC/dpc.pdf*

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

URI *[en]* *https://www.policia.es/certs/AC_DGP_001-SHA1.crt*

URI *[es]* *https://www.policia.es/certs/AC_DGP_001-SHA1.crt*

URI *[en]* *https://www.policia.es/certs/AC_DGP_001-SHA2.cer*

URI	*[es]*	*https://www.policia.es/certs/AC_DGP_001-SHA2.cer*
URI	*[en]*	*https://www.policia.es/certs/AC_DGP_002-SHA1.crt*
URI	*[es]*	*https://www.policia.es/certs/AC_DGP_002-SHA1.crt*
URI	*[en]*	*https://www.policia.es/certs/AC_DGP_002-SHA2.cer*
URI	*[es]*	*https://www.policia.es/certs/AC_DGP_002-SHA2.cer*

2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

2.2.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

2.2.5 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by subordinated CA under the root CA for Public Administration*
Name	*[es]*	*Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP*

Service digital identities

X509SubjectName

Subject CN:	*AC RAIZ DGP*
Subject OU:	*CNP*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*

X509SKI

X509 SK I	*Dpx24aIuiTNB8uM+bFsWRb29ho4=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

2.2.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.2.5.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.2.1.102.36*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.2.1.102.37*

2.2.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.2.6 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by subordinated CA under the root CA for Public Administration*
Name	*[es]*	*Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP*

Service digital identities

X509SubjectName

Subject CN:	*AC RAIZ DGP*
Subject OU:	*CNP*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*

X509SKI

X509 SK I	*Dpx24aIuiTNB8uM+bFsWRb29ho4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-03-17T00:00:00Z*

2.2.6.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.2.6.5 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.2.1.102.36*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.2.1.102.37*

2.3 - Service (granted): Qualified Certificates issued by subordinated CA under the root CA DNIe 2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by subordinated CA under the root CA DNIe 2*

Name *[es]* *Certificados Reconocidos emitido por CAs subordinadas de la CA Root DNIe 2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *573008047581153304165923367944923306 59*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIF2zCCA8OgAwIBAgIQKxu7y2HPSCRSRV09XtviozANBgkqhkiG9w0BAQsFADBfMQswCQYDVQQG
EwJFUzEoMCYGA1UECgwfREISRUNDSU9OIEdFTkVSQUwgREUgTEEgUE9MSUNJQTENMAsGA1UECwwE
RESJRTEXMBUGA1UEAwwOQUMgUkFJWiBETkIFIDIwIHcNMTMwOTI3MTAyNjA1WhcNNDMwOTI3MTAy
NjA1WjBfMQswCQYDVQQGEwJFUzEoMCYGA1UECgwfREISRUNDSU9OIEdFTkVSQUwgREUgTEEgUE9M
SUNJQTENMAsGA1UECwwERESJRTEXMBUGA1UEAwwOQUMgUkFJWiBETkIFIDIwggIiMA0GCSqGSIb3
DQEBAQUAA4ICDwAwggIKAoICAQDbZC/bRfpl/iNzm/3wUrYLfuL2zkzV3laR/Ioc30S5ay3iDyPg
wVbToNaRYKDaXpUVapN2mU8zFkYvbrbCAnzh3M6FaFWc2rPHkAiSLHpS0JwUMDcCOMt0UvQeu1usEc
LXg8vzrr5qo7FQd5ngAZE1y9DZENipNekIVWqspMtK1/txTirO5UGK78MnIKuuB9yjszbnY7Ity6
l1Vj6sUSt8lYzjEt/FFDbJIrbtpihRKFCLOAmeho2qPPwM15DXTwsZsFaU/4+ukd4CCeUbhe5Ruu
Q4+AGQWqj+mUapyMkGhBs6E8WLqVODwxZLrcnusWvJdxvFKeGPTL1aj0FtxiP6Mzs9V1j/buTbFN
Fv3o30AC42wnQQUVzjRsEsu6auCQJbJHdXjtdFZQOixOjzYBU3iDtGQ3mWzmxXOp5DuMHaSobK
0iBDP7ZDtYZwcodmPdjWIM5UaoypAOwGDs6LZdY4UiudRb45f3LuZAngE9F5WxWTK3Gp1Z76b
CzUcZb9HTOG9SYuyx1ZptvOzugAoY5c2cAZ3USO/CFcYfvmNJhaeSosBx6P+Isi0SYgL6ZBaCpVL
DQBb1Lub9rSQWvbFflpdZ6iWUdX4dzAqmJgWN9VKgrOHsW1u4vhoaw3NAdWysjpvdOqq5wzSw49o
Z9uDFNd4cYRr3++vdaoIf3MTvQIDAQABo4GSMIGPMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgEGMB0GA1UdDgQWBBRT3G5ipM4TG3fqb6FapA+ybxLwmzBNBgNVHSAERjBEMEIGBFUdIAAw
OjA4BggrBgEFBQcCARYsaHR0cDovL3BraS5wb2xpY2lhLmVzL2RuaWUvcHVibGljYWNpb25lcy9k
cGMwDQYJKoZIhvcNAQELBQADggIBACEV8svBAISqKrkFuqSIqm0PZv1V8q4RcpYkHKIOjiWM9/s
yHsdH34ShDryAJ2m8/BvYo6aN0KEMz1XAyWhUQTI32D0Dko0Hm29SpqyWFWt6OMpFcp9Db0Oqsik
0ojPNPIu8gVZ6zRZKcGIMdDF56oySwJwdsNFIdGC1WdFdWTksm14KJrEa43IvgSGPpEr8mIV
QqStetoH7mywuA4D3OJbqsyiUDPJ3/UMfY0z6km0j9Ovl9B0LdFvO+T3fLlUrRYXyt4qJEiAI7A5
KKp8S0uYIoWiWPQZG557jeH1XdkCm5jccHbHFA3vyIYcAs0IPGcXjr++rSsa9K0K/cOrPHosCT0
sl2MOV3c25UGZacKVVSWaAGK4aPWwGc1bmGdbhdwi53M2NPOkKC9QNHA+DbK80gmvdCH68DcYQi
JUt2OrYeiGaAZ7j9NRmCWIPxnMwCJqHSpM4FpSjDSibQHTozf+712DXXrYnvVDldIz7KTWdPaa6
R/Lw8ghV9SE65rnOBw8ZTuDEi/9rmN2u0bLlqmoF63FOCZSAQ2Nv4E/Ks7G/TM9k2f4ftYLna/m
GAzXiK5fUl1OpNuZqaSEY/7ia3Nc175+vYnxn2JhlKFbnBgKwP/r4Z2SDvnXFgb7dgQeOg6o10x
VVABIea0t8VETy3SEfmxvLhkGQ3h

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC RAIZ DNIE 2*

Issuer OU: *DNIE*

Issuer O: *DIRECCION GENERAL DE LA POLICIA*

Issuer C: *ES*

Subject CN: *AC RAIZ DNIE 2*

Subject OU:	*DNIE*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*
Valid from:	*Fri Sep 27 12:26:05 CEST 2013*
Valid to:	*Sun Sep 27 12:26:05 CEST 2043*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DB:64:2F:DB:45:FA:65:FE:23:73:9F:FD:F0:52:B6:0B:7E:E2:F6:CE:4C:D5:DE:56:91:FC:8A:1C:DF:44:B9:6B:2D:E2:0F:23:E0:C1:56:D3:A0:D6:91:60:A0:DA:5E:95:15:9E:95:F6:9D:4F:33:16:46:2F:87:A0:80:9F:38:77:33:A1:5A:15:67:36:AC:F1:E4:02:D4:8B:1E:9E:4E:27:05:0C:0D:E0:8E:33:45:2F:41:EB:B5:BA:C1:1E:2D:78:3C:BF:38:AB:E6:AA:3B:15:07:77:9E:00:19:13:5C:BD:0D:91:0D:8A:93:5E:92:55:56:AA:CA:4C:B4:AD:7F:B7:14:E2:AC:EE:54:18:AE:FC:32:72:0A:BA:E0:7D:CA:3B:33:6E:76:3B:22:DC:BA:97:55:63:EA:C5:12:B7:CB:58:CE:31:2D:FC:51:43:6C:92:2B:6E:DA:62:85:12:85:08:B3:80:99:E8:68:DA:A3:CF:C0:CD:79:0D:74:F0:B1:9B:05:69:4F:F8:FA:E9:1D:E0:20:9E:51:B8:5E:E5:1B:AE:43:8F:80:19:05:AA:8F:E9:94:6A:9C:8C:90:68:41:B3:A1:3C:58:BA:95:38:3C:31:64:BA:DC:9E:EB:16:BC:97:71:BC:52:9E:18:F4:CB:D5:A8:F4:16:DC:62:3F:A3:33:B3:D5:75:8F:F6:EE:4D:B1:4D:16:FD:E8:DF:40:02:E3:67:30:9D:04:14:57:38:D1:B0:4B:2E:E9:AB:82:40:96:C9:1D:D5:E3:B5:D1:59:41:08:B1:42:3C:D8:05:42:77:88:3B:46:43:79:96:CE:6C:57:3A:9E:43:B8:C1:DA:4A:86:CA:D2:20:43:3F:B6:43:B5:86:70:72:87:66:3D:D8:D6:94:CE:54:6A:8C:A9:00:EC:06:0E:CE:8B:65:D5:64:21:4B:BF:75:16:F8:E5:FD:CB:B9:90:27:80:4F:45:E5:6C:56:4C:AD:E3:1A:9D:5F:D9:3E:A1:0B:35:1C:65:BF:47:4C:E1:BD:49:8B:B2:C7:56:69:B6:F3:B3:BA:00:28:63:97:36:70:06:77:51:23:BF:08:57:18:7E:F9:8D:26:16:9E:4A:8B:01:C7:A3:FE:21:28:B4:49:88:0B:E9:90:5A:0A:95:4B:0D:00:61:D4:BB:9B:F6:B4:90:5A:F6:C5:7C:8A:5D:67:A8:96:51:D5:F8:77:30:2A:98:98:16:37:D5:4A:82:B3:87:B1:6D:6E:E2:F8:68:6B:0D:CD:01:D5:B2:B2:3A:6F:74:EA:AA:E7:0C:D2:C3:8F:68:67:DB:83:14:D7:78:71:84:6B:DF:EF:AF:75:AA:08:7F:73:13:BD:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*53:DC:6E:62:A4:CE:13:1B:77:E0:87:A1:5A:A4:0F:B2:87:12:F0:9B*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://pki.policia.es/dnie/publicaciones/dpc*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C5:C3:80:EB:92:40:FB:36:A1:6E:15:F5:D6:BA:D0:BF:61:1F:6D:03:F0:EF:24:22:99:19:E7:D2:D8:12:6C:11*

X509SubjectName

Subject CN:	*AC RAIZ DNIE 2*
Subject OU:	*DNIE*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://pki.policia.es/dnie/certs/AC004.crt*
URI	*[es]*	*http://pki.policia.es/dnie/certs/AC004.crt*
URI	*[en]*	*http://pki.policia.es/dnie/certs/AC005.crt*

URI	*[es]*	*http://pki.policia.es/dnie/certs/AC005.crt*
URI	*[en]*	*http://pki.policia.es/dnie/certs/AC006.crt*
URI	*[es]*	*http://pki.policia.es/dnie/certs/AC006.crt*
URI	*[en]*	*http://pki.policia.es/dnie/publicaciones/dpc*
URI	*[es]*	*http://pki.policia.es/dnie/publicaciones/dpc*

2.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.2.2.2.11*
Description		

2.3.4 - History instance n.1 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by subordinated CA under the root CA DNIe 2*
Name	*[es]*	*Certificados Reconocidos emitido por CAs subordinadas de la CA Root DNIe 2*

Service digital identities

X509SubjectName

Subject CN:	*AC RAIZ DNIE 2*
Subject OU:	*DNIE*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*

X509SKI

X509 SK I	*U9xuYqTOExt34IehWqQPsocS8Js=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2015-04-10T00:00:00Z*

2.3.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.4 - Service (granted): Qualified Certificates issued by AC DGP 004

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC DGP 004*
Name	*[es]*	*Certificados cualificados emitidos por AC DGP 004*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*317948126143950900187042261598579730 09*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHlzCCBX+gAwIBAgIQF+t1SpCwD9ZbYuHa+Cc3ETANBgkqhkiG9w0BAQsFADB3MQswCQYDVQQG
EwJFUzEoMCYGA1UECgwtREUiSRUNDSU9lOEdFTkVSQUwgRE1gTEEgUE9MSUNJQTEMMAoGA1UECwwD
Qi05QMRgwFgYDVQRhDA9WQVRFUy1TMjgxNjAxNUgxFjAUBgNVBAMMDUFDIFJBSVogREdQIDIwHhcN
MTgwODAyMTA1MDAyWhcNMzMwODAyMTA1MDAyWjB0MQswCQYDVQQGEwJFUzEoMCYGA1UECgwtRElS
RUNDSU9lOEdFTkVSQUwgREUgTEEgUE9MSUNJQTEMMAoGA1UECwwDQ05QMRgwFgYDVQRhDA9WQVRF
Uy1TMjgxNjAxNUgxEzARBgNVBAMMCkFDIERHUCAwMDQwggIhMA0GCSqGSIb3DQEBAQUAA4ICDwAw
ggIKAoICAQCuDnWXQPYwDK8o3Ry.XoDQRMWcIVLyEnQ8EIRHSuophQEf8I4eTo8dYYhI0PyMRpeq
8o2BhJ0A2uERGoXpihqK1jtH7AmU9sp1NL1GelcRz3B9sQEEaSm4pMkZM2SszkVo8/25KrfZjGS/
CkMzLkqCgooCap2wD+ivnDoxEoMFrVkL1nZLHbnv9RVbdZZ969RlhjoEXcslhi7SqnOpi0lzpEzO
t2yvjY1SJXQdyLR0H0HSVPr5+fj3Hg6iK+98lpz4quteNExuuHqLMFKJPO1VAyEs1tYcmzlmXZc
lQyWbcl99v48IIIm1IL0i8dbGwtBsaS59UZQkkd/NYuH5b+dmpkLt6lcwRwfc1c7O02QhnYpE9A
1agKHwG9hrzV1jgEai+rPPJSEuGOOXrlGXZJheEF3o8FOvhEfTz3+JfnLB5Iy7GCWBs5EtDUajuC
KOXe98GDmBPqIPsBKNCRtXjyLkdV4a2zBG5/CapOkip+agbDvDgWrCo3EFDJsa7t6v7FWgUcgCcv
NRWd62CxA2jr8y9OAis0Brj5fat95k2c1sIFosw/iXJ5T0wOhSl+Qdxu0lO5QMC218vGOqEVEQz9x
i6YZOmt3zS5uXbyScXv4yXwME3gjd5Xf4mqf6C5GfXO9+OmGfS80IDmKaclgAufj5Hg2rpcm0Vo
JhRZzg1/HQIDAQABo4ICIDCCAhwwHQYDVR0OBBYEFA2n5MC015fkdNyGfFL+9N4yYjK8MGsGCCsG
AQUFBwEBBF8wXTAiBggrBgEFBQcwAYYWaHR0cDovL29jc3AucG9saWNpYS5lczA3BggrBgEFBQcw
AoYraHR0cDovL3BraS5wb2xpY2lhLmVzL2NucC9jZXJ0cy9BO1JhaXoyLmNydDAJBgNVHSMEGDAW
gBSTgOWtUvPsZEOKzTOPG2lWHoejGDRMBgNVHSAEERTBDMEEGBFUdIAAwO7A3BggrBgEFBQsCARYr
aHR0cDovL3BraS5wb2xpY2lhLmVzL2NucC9wdWJsaWNhY2lvbmVzL2RwYzASBgNVHRMBAf8ECDAG
AQH/AgEAMA4GA1UdDwEB/wQEAwIBBjCB+gYDVR0fBIHyMIHvMIHsoIHpoIHmhuZodHRwOi8vcGtp
LnBvbGljaWEuZXMvY25wL2NybHMvQVlMLmNybla Bu2zkYXA6Ly9sZGFwLnBvbGljaWEuZXMvQ049
QUlMLENQPUFDITIwIkFIWUyMERHUCUyMDIxT0k9VkFURVMtI2d4MTYwMTVlLE9VPUNOUCxPPURJ
UkVDQ0lPTiUyMEdFTkVSQUwlMjBERSUyMExBJTIwUE9MSUNJQSxDPUVTP2F1dHVcmI0cVJldm9j
YXRpb25MaXN0P2Jhc2U/b2lqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnQwDQYJKoZIhvcN
AQELBQADggIBAAy0UyYLWk8WkcrpQs0rmVuRSKeQmyYN5tH4Zu42jPhF4jhdL7Q1ktHOctnCHA7z
4NdCx/MCZP0p1ur9LNvx2RK/lmYCZ6OgSYsI+01UY/QY3/OTZr2auzBLbmio6sKNPwjzfaI99SB
Kzbn9KMnf/MaP2SbpQIs1S7NBgFQ2Rsy8b84SIdhkzU76jX7Td90Nr6lcpkqPhNYGuXPdpbRp9RtZ
Qmlgi7ywy1KJV5oMg9AiPgWp+vwYK1qUhJQ2h/ZaZJQrH1hHCw1G+dKtDXGFswB5psP9q5U0cIU
wDBzxd8nYJEE97bZuurWfc/CgaF0lkXVCUwUWvhaZhjhAW3mZ+ZTCJ31V+plwI/UTBQVusc2N9R
Qw5dU06gNdGOUczqbLhhBqxeunOdUshsSYedko6fbeIHo2i83qnseCQKisJr9i+dnlZKtwXBcZFi
Sp7eRucyDhk6RzSLUtEzsGKpv3IZIMXdUpzKqYLOcRW9Mr7Z6++N2YBZu7hBIr0f3jg2kJTSg/
LCXjA2MMf/aRFnsw8WBiDuGHO/LBBI6pvMOyxMOD2bMHyXjS5cKizbOro4aciPj2bDB43f7Kb92L
MStACHAauHQT/EgQsum6QwRkf/uC9PVMP3c/ZcKMU/lMNL5MdSU/e6uaB5fROaVYji9U3Eb2kCmR5
iK4jqHHJBZBf

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC RAIZ DGP 2*

Issuer 2.5.4.97: *VATES-S2816015H*

Issuer OU: *CNP*

Issuer O: *DIRECCION GENERAL DE LA POLICIA*

Issuer C: *ES*

Subject CN: *AC DGP 004*

Subject 2.5.4.97: *VATES-S2816015H*

Subject OU: *CNP*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

Valid from: *Thu Aug 02 12:50:02 CEST 2018*

Valid to: *Tue Aug 02 12:50:02 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AE:0E:E5:97:40:F6:30:0C:AF:28:DD:1C:97:A0:34:11:31:67:25:54:BC:84:9D:0F:04:21:11:D2:BA:8A:61:40:47:FC:D
7:87:BF:2E:8F:1D:61:88:48:D0:FC:8C:46:97:AA:F2:8D:81:6C:9D:00:DA:E1:11:1A:B5:E9:8A:1A:8A:D6:3B:47:EC:09:94:F6:CA:75:34:BD:46:78:87:11:CF:70:7D:B1:01:04:69:29:B8:A4:C9:19:33:64:AC:CE:45:68:F3:FD:B
9:2A:B7:D9:8C:64:BF:0A:43:33:2E:4A:82:82:8A:02:6A:9D:B0:0F:E8:AF:9C:3A:31:12:83:05:AD:59:0B:D6:76:4B:1D:B9:EF:E5:15:5B:75:96:7D:EB:D4:65:86:3A:04:5D:CB:25:86:2E:D2:AA:73:A9:8B:42:33:A4:48:8E:B7:
68:EF:8D:8D:52:25:74:1D:C8:B4:74:1D:01:D2:54:FA:F9:F9:F8:F7:1E:0E:A2:2B:EF:7C:96:9C:F8:AA:EB:5E:34:4C:62:B8:78:AA:2C:C1:4A:24:F3:B5:54:0C:84:B1:3B:58:72:6C:E5:99:76:5C:21:0C:96:6D:C2:3D:F6:FE:3C:
20:82:26:D4:82:DF:E8:17:5B:1B:0B:41:B1:AF:12:F5:46:50:92:57:7F:B4:DD:67:1F:98:7E:76:6A:64:2E:DE:88:73:04:70:15:CD:5C:EC:ED:36:42:EC:58:A4:4F:40:D5:A8:0A:1F:01:BD:86:BC:D5:D6:38:04:6A:2F:AB:3C:F2:7
9:12:E1:8E:39:7A:C8:19:76:49:85:E1:05:DE:8F:05:3A:F8:44:7F:5C:F7:F8:97:E7:2C:1E:48:CB:B1:82:58:1B:39:12:D0:D4:6A:3B:82:28:E5:DE:F7:C1:83:98:13:EA:7C:FB:01:28:D0:91:B5:78:F2:2E:47:55:E1:AD:B3:04:6E:7
F:09:AA:4E:92:2A:7E:6A:06:C3:BC:38:16:AC:2A:37:10:50:C9:B1:AE:ED:EA:FE:C5:5A:05:1C:80:27:2F:35:15:9D:EB:60:B1:03:68:EB:F3:2F:4E:02:2B:34:06:B8:F9:7D:AB:7D:E6:4D:9C:D6:21:68:B3:0F:E2:5C:9E:53:D3:
04:21:4A:5F:90:77:1B:B4:94:EE:50:30:2D:B5:F2:F1:8E:A8:45:44:43:3F:71:8B:A6:19:3A:6B:77:CD:2E:70:5D:BF:F2:E5:C5:EF:E3:25:F0:30:4D:E0:8D:DE:57:1F:89:AA:17:A0:B9:19:F8:D7:27:DF:8E:98:67:D2:F3:40:E6:29
:A7:25:80:0B:87:8F:91:E0:DA:BA:5C:9B:45:68:26:14:59:CE:0D:7F:1D:02:03:01:00:01

Subject Key Identifier *0D:A7:E4:C0:B4:D7:97:E4:74:DC:86:7C:52:FE:F4:DE:32:62:32:BC*

Authority Info Access

http://ocsp.policia.es

http://pki.policia.es/cnp/certs/ACRaiz2.crt

Authority Key Identifier *93:80:EB:56:AD:4B:CF:B1:91:0E:2B:34:CE:3C:62:16:1E:87:BF:80*

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://pki.policia.es/cnp/publicaciones/dpc*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://pki.policia.es/cnp/crls/ARL.crl* *ldap://ldap.policia.es/CN=CRL,CN=AC%20RAIZ%20DGP%202,OI=VATES-S2816015H,OU=CNP,O=DIRECCION%20GENERAL%20DE%20LA%20POLICIA,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*6A:D4:3C:81:5C:D8:47:AF:82:B1:80:A2:A0:BD:39:02:B3:52:0E:19:CF:0E:D2:10:D8:00:99:E5:97:42:99:00*

X509SubjectName

Subject CN:	*AC DGP 004*
Subject 2.5.4.97:	*VATES-S2816015H*
Subject OU:	*CNP*
Subject O:	*DIRECCION GENERAL DE LA POLICIA*
Subject C:	*ES*

X509SKI

X509 SK I	*DafkwLTXl+R03IZ8Uv703jJiMrw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-01-15T01:00:00Z

2.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

2.5 - Service (granted): OCSP Responses issued by Autoridad de Certificación AC RAIZ DNIE 2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

Service type description

[en] *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

[es] *A los servicios de estado de validez del certificado que expidan Protocolo de estado de certificados en línea (OCSP) firmaron respuestas y el funcionamiento de un servidor OCSP como parte de un servicio de un proveedor de servicios de confianza que expiden certificados reconocidos.*

Service Name

Name	*[en]*	*OCSP Responses issued by Autoridad de Certificación AC RAIZ DNIE 2*
Name	*[es]*	*Respuestas OCSP emitidas por Autoridad de Certificación AC RAIZ DNIE 2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *573008047581153304165923367944923306 59*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIF2zCCA8OgAwIBAgIQKxu7y2HPSCRSRV09XtviozANBgkqhkiG9w0BAQsFADBfMQswCQYDVQQG
EwJFUzEoMCYGA1UECgwfREISRUNDSU9OIEdFTkVSQUwgREUgTEEgUE9MSUNJQTENMAsGA1UECwwE
RE5JRTEXMBUGA1UEAwwOQUMgUkFJWiBETkFIDIwHhcNMTMwOTI3MTAyNjA1WhcNNDMwOTI3MTAy
NjA1WjBfMQswCQYDVQQGEwJFUzEoMCYGA1UECgwfREISRUNDSU9OIEdFTkVSQUwgREUgTEEgUE9M
SUNJQTENMAsGA1UECwwERE5JRTEXMBUGA1UEAwwOQUMgUkFJWiBETkFIDIwggEiMA0GCSqGSIb3
DQEBAQUAA4ICDwAwggIKAoICAQDbZC/bRfpl/iNzn/3wUrYLfuL2zkzV3laR/Ioc30S5ay3iDyPg
wVbToNaRYKDaXpUVnpX2nU8zFkYvh6CAnzh3M6FaFWc2rPHkAtSLHp5OJwUMDeCOM0UvQcu1usEc
LXg8vzur5qo7FQd3ngAZE1y9DZENipNekIVWqspMtK1/tx TirO5UGK78MnIKuuB9yjszbnY7Itv6
IVYj6sUSi8YzjEzFFDbJIrbipuhRKFCLOAmchn2qPPwM15DXTwsZsFaU/4+ukdkCCcUbhcSRuu
Q4+AGQWqj+mUapyMkGhBs6E8WLqVODwxZLrcnusWvJdxvFKeGPTL1aj0FtxiP6Mzs9V1j/buTbFN
Fv3o30AC42cwnQQUVzjRsEsu6auCQJbJHdXjtdFZQQixQjzYBUJ3iDtGQ3mWzmxXOp5DuMHaSobK
0iBDP7ZDYZwcodmPdjWIM5UaoypAOwGDs6LZdVkIUu/dRb45f3LuZAngE9F5WxWTK3jGp12T6b
CzUcZb9HTOG9SYyxIZptvOzugAoY5c2cAZ5USO/CFcYfvmNJhaeSosBx6P+ISi0SYgL6ZBaCpVL
DQBb1Lub9tSQWvbFfpdZ6oWUdXddzAqmJgWN9VKgrOHsWJu4vhaaw3NAdWysprdfQqg5wzSw49o
Z9uDFNd4cYRt3++vdaoIf3MTvQIDAQABo4GSMIGPMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgEGMB0GA1UdDgQWBBRT3G5ipM4TG3fgh6FapA+yhxLwmzBNBgNVHSAERjBEMEIGBFUdIAAw
OjA4BggrBgEFBQcCARYsaHR0cDovL3BraS5wb2xpY2lhLmVzL2RuaWUvcFHvibGjlYWNpb25icy9k
cGMwDQYJKoZIhvcNAQELBQADggIBACEV8svBAISqKzkFuqSlqm0PZs1V8q4RcpYkHKRfDjrWMt9/s
yHsdH34ShDryAJ2m8/BvYo6aN0KEMz1XAyWhUQTS2D0Dko0FmZ9SpqyWFWf6OMpFcp9Db0Oqsik
0ojPNPloBgVZ6ZcRZKcGlMdDF5fooy5wJ/w0stNFldGC1WdFdWTksmT4KlrEa43lvgSGPgErBnV
QqStetoH7mywuA4D3OJbqsyrL/DPJ3/UMY0z6km0j9Ovl9B0LdFvO+T3fLlUrRYXyf4qJEiAI7A5
Kkg8S0uYIoWiWPQZG557jeH1XdkCm5jcHbIfAJvyIYcAs0lPGcXjr++rSsa9K0KccOrPHosCT0
sl2MOV3c25UGZacKVVSWaAGK4aPWwGc1bnGdbhdwi53M2NPOkKC9QNHA+DbK80gm/dCH68DcYQi
JUtt2OtYeiGaAZ7j9NRmCWIPxnMwCJqlHSpM4FpSjDSihQHToZ+712DXXrYnyVDdl0z7KTWdPaa6
R/Lw8ghV9SE65riOBw8ZTuDEi/9rnN2u0bLIqmoF63FOCZSAQ2Nv4E/Ks7G/TM9k2fHfYLna/m
GAzXfk5fU1OpNuZqsSEY/7ta3Nc175+vYnxn2JJhIKFbnBgKwP/r4Z2SDVnXFgb7dgQeOg6o10x
VVABIea0t8VETy3SEfnxvLhkGQ3h
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *AC RAIZ DNIE 2*

Issuer OU: *DNIE*

Issuer O: *DIRECCION GENERAL DE LA POLICIA*

Issuer C: *ES*

Subject CN: *AC RAIZ DNIE 2*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

Valid from: *Fri Sep 27 12:26:05 CEST 2013*

Valid to: *Sun Sep 27 12:26:05 CEST 2043*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DB:64:2F:DB:45:FA:65:FE:23:73:9F:FD:F0:52:B6:0B:7E:E2:F6:CE:4C:D5:DE:56:91:FC:8A:1C:DF:44:B9:6B:2D:E2:0F:23:E0:C1:56:D3:A0:D6:91:60:A0:DA:5E:95:15:9E:95:F6:9D:4F:33:16:46:2F:87:A0:80:9F:38:77:33:A1:5A:15:67:36:AC:F1:E4:02:D4:8B:1E:9E:4E:27:05:0C:0D:E0:8E:33:45:2F:41:EB:B5:BA:C1:1E:2D:78:3C:BF:38:AB:E6:AA:3B:15:07:77:9E:00:19:13:5C:BD:0D:91:0D:8A:93:5E:92:55:56:AA:CA:4C:B4:AD:7F:B7:14:E2:AC:EE:54:18:AE:FC:32:72:0A:BA:E0:7D:CA:3B:33:6E:76:3B:22:DC:BA:97:55:63:EA:C5:12:B7:CB:58:CE:31:2D:FC:51:43:6C:92:2B:6E:DA:62:85:12:85:08:B3:80:99:E8:68:DA:A3:CF:C0:CD:79:0D:74:F0:B1:9B:05:69:4F:F8:FA:E9:1D:E0:20:9E:51:B8:5E:E5:1B:AE:43:8F:80:19:05:AA:8F:E9:94:6A:9C:8C:90:68:41:B3:A1:3C:58:BA:95:38:3C:31:64:BA:DC:9E:EB:16:BC:97:71:BC:52:9E:18:F4:CB:D5:A8:F4:16:DC:62:3F:A3:33:B3:D5:75:8F:F6:EE:4D:B1:4D:16:FD:E8:DF:40:02:E3:67:30:9D:04:14:57:38:D1:B0:4B:2E:E9:AB:82:40:96:C9:1D:D5:E3:B5:D1:59:41:08:B1:42:3C:D8:05:42:77:88:3B:46:43:79:96:CE:6C:57:3A:9E:43:B8:C1:DA:4A:86:CA:D2:20:43:3F:B6:43:B5:86:70:72:87:66:3D:D8:D6:94:CE:54:6A:8C:A9:00:EC:06:0E:CE:8B:65:D5:64:21:4B:BF:75:16:F8:E5:FD:CB:B9:90:27:80:4F:45:E5:6C:56:4C:AD:E3:1A:9D:5F:D9:3E:A1:0B:35:1C:65:BF:47:4C:E1:BD:49:8B:B2:C7:56:69:B6:F3:B3:BA:00:28:63:97:36:70:06:77:51:23:BF:08:57:18:7E:F9:8D:26:16:9E:4A:8B:01:C7:A3:FE:21:28:B4:49:88:0B:E9:90:5A:0A:95:4B:0D:00:61:D4:BB:9B:F6:B4:90:5A:F6:C5:7C:8A:5D:67:A8:96:51:D5:F8:77:30:2A:98:98:16:37:D5:4A:82:B3:87:B1:6D:6E:E2:F8:68:6B:0D:CD:01:D5:B2:B2:3A:6F:74:EA:AA:E7:0C:D2:C3:8F:68:67:DB:83:14:D7:78:71:84:6B:DF:EF:AF:75:AA:08:7F:73:13:BD:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *53:DC:6E:62:A4:CE:13:1B:77:E0:87:A1:5A:A4:0F:B2:87:12:F0:9B*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://pki.policia.es/dnie/publicaciones/dpc

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C5:C3:80:EB:92:40:FB:36:A1:6E:15:F5:D6:BA:D0:BF:61:1F:6D:03:F0:EF:24:22:99:19:E7:D2:D8:12:6C:11*

X509SubjectName

Subject CN: *AC RAIZ DNIE 2*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

X509SKI

X509 SK I *U9xuYqTOExt34IehWqQPsocS8Js=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-04-21T00:00:00Z

2.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3 - TSP: Agencia Notarial de Certificación S.L. Unipersonal

.

TSP Name

Name	*[en]*	*Agencia Notarial de Certificación S.L. Unipersonal*
Name	*[es]*	*Agencia Notarial de Certificación S.L. Unipersonal*

TSP Trade Name

Name	*[en]*	*VATES-B83395988*
Name	*[en]*	*ANCERT - Agencia Notarial de Certificación*
Name	*[es]*	*ANCERT - Agencia Notarial de Certificación*
Name	*[en]*	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Name	*[en]*	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

PostalAddress

Street Address	*[en]*	*Paseo General Martínez Campos, 46*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28010*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Paseo General Martínez Campos, 46*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28010*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:ancert@ancert.com*
URI	*[en]*	*http://www.ancert.com*

TSP Information URI

URI	*[en]*	*http://www.ancert.com/en*
URI	*[es]*	*http://www.ancert.com*

3.1 - Service (withdrawn): Certificados Corporativos Personales v.2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Corporativos Personales v.2*
Name	*[en]*	*Personal Corporate Certificate v2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *825184943542858205923177230689866848 96*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHsjCCBa6gAwIBAgIQPbR74nXzs3KUtaDbZKXI4DANBgkqhkiG9w0BAQsFADCBgDELMAkGA1UE
BhMCRVMxQTAzBgNVBAoTOEFnZWS5aWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2lvbiBTLkwuVS4g
LSBDSUYgQjgzMzK1OTg4MS4wLAYDVQQDEyVBTkNFUlQgQ2VydGlmaWNhZG9zIFJlZGVzIFByaXZh
ZGFzIFYyMB4XDTE2MDYyMTEwMDkzMloXDTMwMDUyNTAwMDEwMFowgcIxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHEztQYXNlbyBkZWwgR2VuZXJhbCBNYXJlIuW5leiBlDYW1wb3MgNDYgNmEgcGxhbnRhID4
MDEwIE1hZHJpZDFBMD8GA1UEChM4QWdlbmNpYSBC0b3RlcmlhbCBkZSBlZXL0aWZpY2EjaW9uIFMu
TC5VL1AtIENRiBCODMzOTU5ODgxKjAoBgNVBAMTIUFOQ0VSVCBDb3Jwb3JhdGl2b3MgUGVyc29u
YWxlcyBWMjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK8cgvcy9dXGFtR5l4AhIaH0
RVCUu7Xl/x7X6X8FADGmbenNc/ubHsElrTHBrqIgWkJTd8P1oydSfoDIxIllmdpzFxWsHIOz3VH
xuNE8/pvWmQDfbaSFNZzn0xyFgGp/95wG+zoG28lGGykIy6LAqJ2KAwKUCZLZC9PnPdstNaWHz
bAWm8Pj5kpJ2l3PCXZ/aar6l4ymYgPwpB+1WrY2H/hzqK0pnByVad6mUrRqKfCNlwgkUNl9qWKFp
vqN1jik6zC8hzHJ8RL0FDLDsii327FUh5POQtXX4npulwYr+m7Mqixh1NruEjB37r+1/o7rzWfV2
cMMxR9cdJi10llfwzGA0mfiIhBAaCjKZTYBCht8rtbykbKC4xP/4DrIDZ26bVhmhtAyqidvnfnDV
Vj3Kd8QoAcM8esJdw71+0LdeC9k6VcQZ0FoZYTdIYmyz7antu7U13wuOYAJNdzLx95gnI1YHAW
3Ge1IMhP7c1N3SEpTRRigKt533uKtjN+vKOLQxaUf7JmwILWSCDx/o+eCK0SBOLs5kdYiRM/eaWs
bn/DjE+h+CBhr2ibVmJk4eqgrssWINSI9l/sT3ikedjmX09X+x64Dythxb9JqqGbQVRwwmRtyyah
be0PWOuMKyr80hHLm/iSCYz90LJ2mNa5x+GMtG2WXZAXJVYfjbBVAgMBAAGjggH2MIIB8jCBgQY1
KwYBBQUHAQEEdTBzMC8GCCsGAQUFBzABhiNodHRwOi8vb2NzcC5hYy5bbmNlcnQuY29tL29jc3Au
eHVkYTBABggrBgEFBQcwAoY0aHR0cDovL3d3dy5bbmNlcnQuY29tL3BraS92Mi9jZXJ0cy9BTkNF
UlRQUklWX1YyLmNydDAfBgNVHSMEGDAWgBT9PGp5ZhU8ALvSNqJipljmGuAzrzASBgNVHRMBAJ8E
CDAGAQH/AgEAMEEGA1UdIAQ6MDgwNgYKKwYBBAGBk2gCATAoMCYGCCsGAQUFBwIBFhpodHRwczov
L3d3dy5bbmNlcnQuY29tL2NwczCBnQYDVR0fBIGVMIGSMIGPoIGMoIGJhitodHRwOi8vd3d3LmFu
Y2VydC5jb20vY3JsL0FOQ0VSVFBSSVZfVjIuY3lsbxcdHRwOi8vd3d3Mi5bbmNlcnQuY29tL2Ny
bC9BTkNFUlRQUklWX1YyLmNybHYsaHR0cDovL3d3dzMuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUUFJJ
V19WMi5jcmwwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBRl7t0pAwFDacgePVuBfqXzoXas+DAI
BgNVHREEHjAcgRpwa2kuZXhwbG90YWNpb25AYW5jZXJ0LmNvbTANBgkqhkiG9w0BAQsFAAOCAgEA
bDXRohcMvnYceWYv/4u/sPfs2l0mE1660wgDqwsMbfUTFv5QVOjCumvzzkbc7NZ37T+Gd3UEtnaF
q4VITCBKnVXnCFna8y15QFh4G0LSaOCHtB86SBxpMIE+DKCDfE78DmoNV9x361aeARxTSRufUGj9
2ceyP73crSrGzBLaTCluUiLS2BjUeY0Pv7tEdy0mjhLmWVOY+qdTgOv+GWDNzKKSb8/xmYxhi239
fB34cRP7BBK6BnL/3ylb4tv8oOTamjRzCpCVpGdB6g33QE9ooBj5bDQMedCdN5me97X/+plFCm
YtXLFukEd6Jk9grRTGvDP9IHgcL1luvWs22stQ79IwrMImmqDrUQboRanWu52HMDkjHlcsGyyE
eCwSuhvreu/wW98Qy+eNhbGvUlSkd1dsATob0/hDO0/yJiYfVWTdwtSVwb1+wbNfK6F+NzLhmoZU
HrOwz0ECOOjo4/r9ZVB2vUHlNgvHpRnkMAzQopEYdbit TWg4ehvXwAXWPMOHyvtiFZNNTVcz1lcs
fiDYFgBugNxCK1Tl3diOGBaSMcMTpWM6zg5O5/le2PsrLNE1RI/Lb6O9oLxofz51q9QMbp17zRCw
R/cC3aFy2NCBw9XgSiA/itbahlvLnLuAViUV6XJfz2hJMiHExr7y9XtkbqBQFW6sq5XFmYvxHwk=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ANCERT Certificados Redes Privadas V2*
Issuer O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Issuer C:	*ES*
Subject CN:	*ANCERT Corporativos Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Tue Jun 21 12:09:32 CEST 2016*

Valid to: *Sat May 25 02:01:00 CEST 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AF:1C:82:F7:32:F5:D5:C6:16:D4:79:97:80:21:21:A1:F4:45:50:94:BB:B5:E5:FF:1E:D7:E9:7F:05:00:31:A6:6D:E9:C:D:73:FB:9B:1E:C1:25:AD:31:C1:AE:A2:20:5A:42:53:77:C3:F5:A3:FC:9D:49:FA:03:23:12:25:86:67:69:CC:5C:36:C4:72:0E:CF:75:47:C6:E3:44:F3:FA:6F:5A:64:03:7D:B6:92:14:D6:73:9F:4C:72:16:01:A9:FF:DE:70:1B:EC:E8:1B:6F:25:18:6C:A4:D7:2E:8B:02:3A:B5:D8:A0:30:29:40:99:2F:F6:42:F4:F9:CF:76:CB:4D:69:61:F3:6C:05:A6:F0:F8:F9:92:92:76:23:73:C2:5D:9F:DA:6A:BE:A5:E3:29:98:80:FC:29:07:E8:96:AD:8D:87:FE:1C:EA:2B:4:A:67:07:25:5A:77:A9:94:AD:1A:8A:7C:23:65:C2:09:14:36:5F:6A:58:A1:69:BE:A3:75:8E:29:3A:CC:2F:21:CC:72:7C:44:BD:05:0C:B0:EC:8A:2D:F6:EC:55:21:E4:F3:90:B5:75:F8:9E:9B:A5:C1:8A:FE:9B:B3:2A:8B:18:75:3:6:BB:84:8C:1D:FB:AF:E2:3F:A3:BA:F3:59:F5:76:70:C3:31:47:D7:1D:26:22:34:96:57:F0:CC:60:34:99:F8:9F:84:10:1A:0A:32:99:4D:80:42:86:DF:2B:B5:BC:A4:6C:A0:B8:C4:FF:F8:0E:B9:43:67:6E:A1:56:19:A1:B4:0C:AA:89:DB:E7:7E:70:D5:56:3D:CA:77:C4:28:03:13:3C:7A:F2:5D:C1:3D:7E:D0:B7:5E:0B:DF:E4:E9:57:90:67:41:68:65:84:DD:21:89:F2:CF:BB:A7:B6:EE:D4:D7:7C:2E:39:80:09:FC:DE:31:2F:1F:79:82:77:F5:60:70:16:DC:67:B5:20:C8:4F:ED:CD:4D:DD:21:29:4D:14:62:80:AB:79:DE:CB:8A:B6:33:7E:BC:A3:8B:43:16:94:23:B2:66:C2:52:D6:48:20:F1:FE:8F:9E:08:AD:12:04:E2:EC:E6:47:58:89:13:3F:79:A5:AC:6E:7F:C3:8C:4F:A1:F8:20:61:AF:68:9B:56:62:64:E1:EA:A0:AE:CB:16:20:D4:A5:F6:5F:EC:4F:78:A4:79:D8:E6:5F:4F:57:FB:1E:B8:0F:2B:61:C5:BF:49:AA:A1:9B:41:54:70:C2:64:6D:CB:26:A1:6D:EB:4F:58:EB:8C:2B:2A:FC:D2:11:CB:9B:F8:92:09:8C:FD:D0:B2:76:98:D6:B9:C7:E1:8C:B4:6D:96:5D:90:17:25:56:1F:8E:10:55:02:03:01:00:01

Authority Info Access

http://ocsp.ac.ancert.com/ocsp.xuda

http://www.ancert.com/pki/v2/certs/ANCERTPRIV_V2.crt

Authority Key Identifier *FD:3C:6A:79:66:15:3C:00:BB:D2:36:A2:62:A6:58:E6:1A:E0:33:AF*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.2.1

CPS pointer: https://www.ancert.com/cps

CRL Distribution Points

http://www.ancert.com/crl/ANCERTPRIV_V2.crl

http://www2.ancert.com/crl/ANCERTPRIV_V2.crl

http://www3.ancert.com/crl/ANCERTPRIV_V2.crl

Subject Key Identifier *5F:EE:DD:29:03:01:43:69:C8:1E:3D:5B:81:7E:A5:F3:A1:76:AC:F8*

Subject Alternative Name *pki.explotacion@ancert.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AE:9E:FF:CD:7B:83:0D:9A:7A:6D:F0:90:7E:DF:CE:FE:5D:C8:8A:A5:CC:B7:04:5F:03:FD:67:1C:BD:E5:B4:B7*

Certificate fields details

Version: *3*

Serial Number: *151806557225635609738953006987710450500*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHOjCCBSggAwIBAgIQcjThImyLg1wyzvn9BtpLRDANBgkqhkiG9w0BAQsFADCBgDELMAkGA1UE
BhMCRVMxQTAzBgNVBAo7OUEnZWS5jaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2ibyBTLkwuVS4g
LSBDSUYgQjgzMzk1OTg4MS4wL.AYDVQQDEyVBTkNFUlQgQ2VydGlmaWNhZG9zIFJlZGVzIFByaXZh
ZGFzIFYyMB4XDTEwMDUyNzA3NDYzNFoXDTIwMDUyNzA3NDYzNFowgcIxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHEztQYXNlbyBkZWwgR2VuZXJlbCBNYXJ0aW5lcIDYW1wb3MgNDYgNmEgcGxhbnRhIDI4
MDEwIE1hZHIpZDFBMD8GA1UEChM4QWdlbmNpYSB0b3Rhcmlhbi5BZSBlZXlBaWVpYY2FjaW9uIFMu
TCSVLzAxIEN3RzR0CODMzOTU5ODgxKjAoBgNVBAMTIUFOQ0VSVCBlZDb3Jwb3JhdGl2b3MgLGVyc29u
YWxlcyBWMjCCAiwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK8cgvcy9dXGFtR5l4AhIaH0
RVCUu7Xl/x7X6X8FADGmbenNc/ubHsElrTHBrqIgWkJTd8P1o/ydSfoDIxIlhmdpzFxWxHIOz3VH
xuNE8/pvWmQDfbaSFNZzn0xyFgGjp/95wG+zoG28lGcyk1y6LAjq12KAwKUCZL/ZC9PnPdstNaWHz
bAWm8P/5kpI2f3PCX2/aar6l4ymYgPnpB+WrY2H1hzqK0pnByVad6mUrRqKfCNlwgkUN9qWKFp
vqN1jik6zC8hzHJ8RL0FDLDsii327FUh5POQtXX4npuhvYr+m7Mqixh1NruEjB37r+1o7rzWIV2
cMMxR9cdJi10IlfwzGA0mfiIhBAaCjKZTYBCht8rtbykbKC4xP/4DrlDZ26bVhmhtAyqidvnfnDV
Vj3Kd8QoAxM8evJdwT1+0LdeC9ke6VeQZ0FoZYTdIYnyz7untu7U13wuOYAUN4xLx95gnf1YHAW
3Gc1MbP7c1N3SEp7RRtgKz55suKtjN+vkO0LQsaUT/mwIL WSCDx/o+eCK0SB0LsSkdYiRMceaWs
bn/DjE+h+CBhr2ibVmJk4eqgrssWINSl9l/s73ikedjmX09X+x64Dythxb9JqGbQVRwwmRtyyah
betPWOuMKyr80hHLm/iSCYz90LJ2mNa5x+GMtG2WXZAXJVYfjhBVAgMBAAGjggFyMIIBbjAfBgNV
HSMEGDAWgBT9PGp5ZhUSALvSNqJiplmGuAzrzASBgNVHRMBAf8ECDAGAQH/AgEAMEEGA1UdIAQ6
MDgwNgYKKwYBBAGBk2gCATAsMCYGCCsGAQUFBwIBFhpodHRwczovL3d3dy5hbmNlcnQuY29tL2Nw
czCBnQYDVR0fBIGVMIGSMIGPoIGMoIGJhitodHRwOi8vd3d3LmFuY2VydC5jb20vY3JsL0FOQ0VS
VFBSSVZlVjluY3JshixodHRwOi8vd3d3Mi5hbmNlcnQuY29tL2NybC9BTkNFUlRQUkJWX1YyLmNy
blYsaHR0cDovL3d3dzMuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUUFJVI9WMi5jcmwwDgYDVR0PAQH/
BAQDAgGGMB0GA1UdJgQWBBRl70pAwFDacgePVuBfqXzoXas+DAIBgNVHREEHjAcgRpwa2kuZXlw
bG90YWNpb25AYW5jZXJ0LmNvb TANBgkqhkiG9w0BAQsFAAOCAgEAQFqE/EKHzfuWWt8H1e9tcaPw
PlEJJ+OxwE566Wrqk0rpjx7ptRtujb1jAJ8FPd5dBSuvksGaF5xx0NGurcOPrQ2ceejM9urnlvSWu
EDSEpSGpVktNQ+EcD8SxiUlugs/MNXcNalHsiuszWcmca7F3akHB5JJ/dC7T1EyGnZAw/JaXTS4l
9EWVIBJhpPfIso1HrKb66HuBauQclwy4JP+iIKE2jRtjFreHXEVXPwcWE4CnSIWyqLXCjHeyxaOJ
AsPcZN4wjo8PPdFbZMsMbHujDugnYuhkV01uV3WwGJcrCOX3kazXr8T/RAcMkx8ooSa52o39
2Yrd0v8xcBi9hXGyv8Y5/iojvp8yh4PYt8Uca/B9N7Hmfnl4qcB7cqyk+XolplzE/FZzaPWcdv+jc
IMCqdWiNntnWDA1i5CO874/TRhX9Hc5CVeFt10IM9wUAJjtL Ih/h0dN2pm/txwBGWoeG4o0HVN0L
wlmrbJ9xij1MCmzuoaKKNOQtMDjio5Fa16O92vtaibrPIkjxXlCGKlCuCMJsouGPzODs2kmKFm7
vzKyqnpktWSon17QpX2jg5wcoyB+aA57tbF/XztR8H7c3G86cXTf56Selj+BgyymNzb9bv0KLj6
z0aDlE5tcL6Hw61bCaLSutB1QUcJRX2Ay+i1dtN6kXo2ihKgc8=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Certificados Redes Privadas V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Corporativos Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Thu May 27 09:46:34 CEST 2010*

Valid to: *Wed May 27 09:46:34 CEST 2020*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AF:1C:82:F7:32:F5:D5:C6:16:D4:79:97:80:21:21:A1:F4:45:50:94:BB:B5:E5:FF:1E:D7:E9:7F:05:00:31:A6:6D:E9:C
D:73:FB:9B:1E:C1:25:AD:31:C1:AE:A2:20:5A:42:53:77:C3:F5:A3:FC:9D:49:FA:03:23:12:25:86:67:69:CC:5C:56:C4:72:0E:CF:75:47:C6:E3:44:F3:FA:6F:5A:64:03:7D:B6:92:14:D6:73:9F:4C:72:16:01:A9:FF:DE:70:1B:EC:
E8:1B:6F:25:18:6C:A4:D7:2E:8B:02:3A:B5:D8:A0:30:29:40:99:2F:F6:42:F4:F9:CF:76:CB:4D:69:61:F3:6C:05:A6:F0:F8:F9:92:92:76:23:73:C2:5D:9F:DA:6A:BE:A5:E3:29:98:80:FC:29:07:E8:96:AD:8D:87:FE:1C:EA:2B:4
A:67:07:25:5A:77:A9:94:AD:1A:8A:7C:23:65:C2:09:14:36:5F:6A:58:A1:69:BE:A3:75:8E:29:3A:CC:2F:21:CC:72:7C:44:BD:05:0C:B0:EC:8A:2D:F6:EC:55:21:E4:F3:90:B5:75:F8:9E:9B:A5:C1:8A:FE:9B:B3:2A:8B:18:75:3
6:BB:84:8C:1D:FB:AF:E2:3F:A3:BA:F3:59:F5:76:70:C3:31:47:D7:1D:26:22:34:96:57:F0:CC:60:34:99:F8:9F:84:10:1A:0A:32:99:4D:80:42:86:DF:2B:B5:BC:A4:6C:A0:B8:C4:FF:F8:0E:B9:43:67:6E:A1:56:19:A1:B4:0C:AA
:89:DB:E7:7E:70:D5:56:3D:CA:77:C4:28:03:13:3C:7A:F2:5D:C1:3D:7E:D0:B7:5E:0B:DF:E4:E9:57:90:67:41:68:65:84:DD:21:89:F2:CF:BB:A7:B6:EE:D4:D7:7C:2E:39:80:09:FC:DE:31:2F:1F:79:82:77:F5:60:70:16:DC:67:
B5:20:C8:4F:ED:CD:4D:DD:21:29:4D:14:62:80:AB:79:DE:CB:8A:B6:33:7E:BC:A3:8B:43:16:94:23:B2:66:C2:52:D6:48:20:F1:FE:8F:9E:08:AD:12:04:E2:EC:E6:47:58:89:13:3F:79:A5:AC:6E:7F:C3:8C:4F:A1:F8:20:61:AF:
68:9B:56:62:64:E1:EA:A0:AE:CB:16:20:D4:A5:F6:5F:EC:4F:78:A4:79:D8:E6:5F:4F:57:FB:1E:B8:0F:2B:61:C5:BF:49:AA:A1:9B:41:54:70:C2:64:6D:CB:26:A1:6D:EB:4F:58:EB:8C:2B:2A:FC:D2:11:CB:9B:F8:92:09:8C:F
D:D0:B2:76:98:D6:B9:C7:E1:8C:B4:6D:96:5D:90:17:25:56:1F:8E:10:55:02:03:01:00:01

Authority Key Identifier *FD:3C:6A:79:66:15:3C:00:BB:D2:36:A2:62:A6:58:E6:1A:E0:33:AF*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.2.1

CPS pointer: https://www.ancert.com/cps

CRL Distribution Points

http://www.ancert.com/crl/ANCERTPRIV_V2.crl

http://www2.ancert.com/crl/ANCERTPRIV_V2.crl

http://www3.ancert.com/crl/ANCERTPRIV_V2.crl

Subject Key Identifier *5F:EE:DD:29:03:01:43:69:C8:1E:3D:5B:81:7E:A5:F3:A1:76:AC:F8*

Subject Alternative Name *pki.explotacion@ancert.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8A:C2:CF:DE:0B:8A:60:12:51:8A:A3:BC:EF:89:55:26:B1:A5:29:B4:F6:39:54:4B:23:2C:DD:62:8D:81:5D:71*

X509SubjectName

Subject CN: *ANCERT Corporativos Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-02-15T01:00:00Z*

3.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Corporativos Personales v.2*

Name *[en]* *Personal Corporate Certificate v2*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Corporativos Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

X509SKI

X509 SK I *X+7dKQMBQ2nIHj1bgX6l86F2rPg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

3.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Corporativos Personales v.2*

Name *[en]* *Personal Corporate Certificate v2*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Corporativos Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

X509SKI

X509 SK I *X+7dKQMBQ2nIHj1bgX6l86F2rPg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-11-16T00:00:00Z*

3.2 - Service (withdrawn): Certificados Personales de Corporaciones de Derecho Público v.2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Personales de Corporaciones de Derecho Público v.2*

Name *[en]* *Qualified Personal Certificates for Public Corporations v2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *94162850161103275073603007908394695622*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHZzCCBcOgAwIBAgIQRtca83XgXiUnyycugQH7xjANBgkqhkiG9w0BAQsFADCBbTELMAkGA1UE
BhMCRVMxQTAyBgNVBAoTOEFnZWSjaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2lvbnBTLkwuVS4g
LSBDSUYgQjgzMzk1OTgsMTMwMQYDVQQDEypBTkNFUlQgQ29yc0YyWNpb25lcyBkZSBEZXJlY2hv
IFB1YmxpY28gVjIwHhcNMTYwNjIxMTAxNjI2WhcNMzAwNTI1MDAwMTAwWjCB1jELMAkGA1UEBhMC
RVMxRDBCBgNVBAcTO1Bhc2VvIGRlbCBHZW5lcmFsIE1hcnRpbmV6IENhbXBvcyA0NiA2YSBwbGFu
dGEgMjgwMTAgTWFkcmlkMUEwPwYDVQQKEzhBZ2VuYzlhIE5vdGFyaWFsIGRlIENlcnRpZmlyYWNp
b24gIy5MLUulC0gQ0lGIE4MzM5NTk4ODE=MDAwGA1UEAxM1QUSDRVJUIENvcnBvcmFjaWNuZXMg
ZGUgRGVyZWNobyBQdWJsaWNvIFBlcnNvbmFsZXMgVjIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAw
ggIKAoICAQCdLUMJ5mVrg6bL16IDQ7G/ytR0b+g69kVoq3lMTVZ3EeVlxLQEABHRZFb2nqazpjZC
PzIS8ycSYaJQouccZRvGiePuxioVHK4l79TuW7iPnRMJ5E7ucxFtxVioQHlOwvuEcaZkqSK8Qlo7
URH5zTsavs6lQnWQFshZQzDLLpsR8f0LDgPbX+kmYdAhapPZTRYnmlBOM6+iPWxmjTaR7zWpLat
k3dTIS9lk+xBbWH+lsbLx8d19cvLD2aiGmaOVpV8AtNfQ/+UKurqbv7gs9WKEfmnX8nKMM6lOlqT
XNEgMHlLVeGYBkBawJzNp1nxwpxHa2tMzWPzt4Hlx1CrM51LD4tKOC0rGyrwC5n5nvs8BnduF0+2
3ex5i7mwTBc60u1zrwVzIwZkm+42ns+POPWGRwDEJ8tWNmAG2j107rqndcWf0AzFsf+nYM/R+Tui
+8evyQq9egFHWM6QleMwcvwwVVUu0tGRUHpJMKJv8KPQycZc9cGI2bg9z3L5W9f6a8uzqCr6eyc
0koMcdhWFs4uHKonGkQZ94seR0WmA7K5dedf/TISoxWjIVZfJBa/LnvMJk4nK6cnm2spUj+gtQLz
9l6N2jjuM8m4/onlIBP18sU31rv6sXsXYxxwzLnW98XCQWpiiU1/CjASszZs01il7/Nx+J3TvpB
ocRL/bwnNQIDAQABo4IB8jCCAc4wgYAGCCsGAQUFBwEBBHQwcjAvBggrBgEFBQcwAYYjaHR0cDov
L29jc3AuYWMuYW5jZXJ0LmNvbS9vY3NwLnh1ZGEwPwYIKwYBBQUHMAKGM2h0dHA6L y93d3cuYW5j
ZXJ0LmNvbS9wa2kvdjIvY2VydHMvQUSDRVJUUFVCX1YyLmNvdDAfBgNVHSMEGDAWgBRAyHOAOVxC
fwhDw9zH9e6A703+2TASBgNVHRMBAf8ECDAGAQH/AgEAMEEGA1UdIAQ6MDgwNgYKKwYBBAGBk2gD
ATAoMCYGCCsGAQUFBwIBFhpodHRwczovL3d3dy5hbmNlcnQuY29tL2NwczCBmgYDVR0fBIGSMIGP
MIGMoIGJoIGGhipodHRwOi8vd3d3LmFuY2VydC5jb20vY3JsL0FOQ0VSVFBVQl9WMi5jcmyGK2h0
dHA6Ly93d3cyLmFuY2VydC5jb20vY3JsL0FOQ0VSVFBVQl9WMi5jcmywGDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBTA
Y2VydC5jb20vY3JsL0FOQ0VSVFBVQl9WMi5jcmwwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBTA
uro3O0NyChxbOzbWst4t9kt8yDAIBgNVHREEHjAcgRpwa2kuZXhwbG90YWNp625AYW5jZXJ0LmNv
bTANBgkqhkiG9w0BAQsFAAOCAgEAadJVDpU/LpMtAvWOa+0yKpttxaaDycqE3I1KueX2Cl6rwYft
QekL1SwWt0lG7hE/AAKfM7tCdykJqMAlgBIqOmGVt+1mtNTbU5O2zs5tH6bY2StIzAlwdsmiq5Od
uubqfGFX5thKdqTbvwd8pZ8aGke4XetEKW+3w+3Z1+E0v0vP+GNWYOV28D/Rvf7eYG9PejNgiT0a
GkSJj9/DwWnNzWkOCXVFDRwx1wOBP2nLOCFpoTFFubtQsDSsL T/R1Oz4t18QJbo0YH7WdSkg7oV2
av35cnCxCzbZ9E8iZFn/uk1tmTJb4fQUHe1D3yULUPZO7O45xWLuPdoo8wg+UNxco/QdNcxhhd0
uYLUaQhiaUCelbcRTXv7CR2JKpOAdF2VP6wm7C15dDSkD80PnysLw7PbX7NRc2Zb/iqJRFP88rs
OY54D/gPl/ohqIBaWOc7oVw2SHqjtWarqC7qpFba7JFPLDxkV+MGjHUaiU7AfcxhsB7YZM9Kxfo
fL e4kKdJl0RglwnnMhIel9ugt+nKkiU/aRbEYPeaR3K41WOIfoqwmNsJ/PVLkfmt8tInJbDCMUa0/z
lfAx2XcRUGuty+St2g+ojSwri9lKj7cXSY7rvESzFWJoR62kMctM5Js5nXg9nqWWPHIGk1By0Q04
bztA4rt5+en58XtH0NwyC0L4Xhg=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Corporaciones de Derecho Publico V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Corporaciones de Derecho Publico Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Tue Jun 21 12:16:26 CEST 2016*

Valid to: *Sat May 25 02:01:00 CEST 2030*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9D:2D:43:09:E6:65:6B:83:A6:CB:97:A2:03:43:B1:BF:CA:24:74:6F:E8:3A:F6:45:68:AB:72:0C:4D:56:77:11:E5:65:C
4:B4:04:00:11:D1:64:56:F6:9E:A6:B3:A6:36:42:3F:32:12:F3:27:12:61:A2:50:A2:E7:1C:65:1B:C6:89:E3:EE:C6:2A:15:1C:AE:25:EF:D4:EE:5B:B8:8F:9D:13:09:E4:4E:EE:73:11:6D:C5:58:A8:40:79:50:C2:FB:84:71:A6:64:A
9:22:BC:40:8A:3B:51:11:F9:CD:3B:1A:BF:A2:10:9D:64:05:B2:1D:90:FF:30:CB:2E:9B:11:F1:F3:8B:0E:03:DB:5F:E9:26:61:D0:21:6A:93:D9:4D:16:27:8A:69:41:38:CE:BE:88:F5:B1:9A:34:E7:47:BC:D6:A4:B6:AD:93:77:5
3:7D:2F:65:93:EC:41:6D:61:FE:22:C6:CB:C7:C7:75:F5:CB:CB:0F:66:A2:1A:66:8E:56:95:7C:02:D3:5F:43:FF:94:2A:EA:EA:6E:FE:E0:B3:D5:8A:7C:99:A7:5F:C9:CA:30:CE:A5:3A:5A:93:5C:D1:20:30:79:4B:55:E1:98:06:
40:5A:C0:9C:CD:A7:59:F1:C2:9C:47:6B:6B:4C:CD:63:F3:B7:81:E5:C7:50:AB:33:9D:4B:0F:8B:AA:38:2D:2B:1B:2A:F0:0B:99:F9:9E:FB:3C:06:77:6E:17:4F:B6:DD:EC:79:8B:B9:B0:4C:17:3A:D2:ED:73:AF:05:73:23:06:6
4:9B:EE:36:9E:C7:8F:38:F5:86:47:00:C4:27:CB:56:36:60:06:DA:3D:74:EE:BA:A7:75:C5:9E:39:AC:C5:B1:FF:A7:60:CF:D1:F9:3B:A2:FB:C7:AF:C9:0A:BD:7A:01:47:58:CE:90:95:E3:30:7A:FC:30:55:5F:D4:BB:4B:46:45:
41:E9:24:C2:89:BF:C2:8F:43:27:19:73:D7:06:7F:66:E0:F6:0D:CB:E5:6F:5F:E9:AF:2E:CE:A0:AB:E9:EC:9C:D2:4A:0C:71:D8:56:15:EE:2E:1C:AA:22:1A:44:19:F7:8B:1E:44:E5:A6:03:B2:B9:75:E7:54:4F:54:A8:C5:68:C9:5
5:99:62:24:16:BF:2E:7B:CC:26:4E:27:2B:A7:27:9B:6B:29:52:3F:A0:89:02:F3:F4:8E:8D:DA:38:EE:33:C9:B8:FE:89:E5:94:13:F5:F2:C5:37:D6:BB:FA:B1:7B:17:63:1C:70:CC:B9:D6:F7:C5:C2:41:6A:62:89:4D:7F:0A:30:12:
B3:36:6C:D3:58:88:EF:F3:71:F8:9D:D3:BF:FA:41:A1:E4:4B:FD:BC:27:35:02:03:01:00:01
```


Authority Info Access

http://ocsp.ac.ancert.com/ocsp.xuda

http://www.ancert.com/pki/v2/certs/ANCERTPUB_V2.crt

Authority Key Identifier *40:C8:73:80:39:5C:42:7F:08:43:C3:DC:C7:F5:EE:80:EC:ED:FE:D9*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.3.1

CPS pointer: https://www.ancert.com/cps

CRL Distribution Points

http://www.ancert.com/crl/ANCERTPUB_V2.crl

http://www2.ancert.com/crl/ANCERTPUB_V2.crl

http://www3.ancert.com/crl/ANCERTPUB_V2.crl

Subject Key Identifier *C0:BA:BA:37:3B:43:72:09:BC:5B:3B:36:D6:B2:DE:2D:F6:4B:7C:C8*

Subject Alternative Name *pki.explotacion@ancert.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *5C:89:A0:A3:04:CD:09:0A:E4:97:C5:9D:90:38:C4:31:E2:36:28:34:31:B9:08:E1:5E:12:4F:94:3A:B0:4A:58*

Certificate fields details

Version: *3*

Serial Number: *135466428519879488225880736606914916039*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHWDCCBUCgAwIBAgIQZemilt402mzqSNMKuryuxzANBgkqhkiG9w0BAQsFADCBbTELMAkGA1UE
BhMCRVMxQTA/BgNVBAoTOEFnZW5jaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2lvbiBTLkwuVS4g
LSBDSUYgQjgzMzK1OTg4MTMwMQYDVQQDEypBTkNFUlQgQ29ycG9yYWNpb25lcyBkZSBEZXJlY2lv
IFB1YmxpY28gVjIwHhcNMTAwNTI3MDgwNDU1WhcNMjAwNTI3MDgwNDU2WjCB1jELMAkGA1UEBhMC
RVMxRlDBC8gNVBAc1O1Bic2VvIGRlbCBlZW5lcmFsIE1henRpbmVóIENhbXBvcyA0NiA2YSBwbGFu
dGEgMjgwMTAgTWFkcmlkMUIwPwYDVQQKEzhDZ2VuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlyYWNp
b24gU y5MLlUuIC0gQ0lGIEl4MzM5NTk4ODE+MDwGA1UEAxM1QU5DRVJUIENvcnBvcmFjaW9uZXMg
ZGUgRGVyZWNobyBQdWJsaWNvIFBlcnNvbmFsZXMgVjIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAw
ggIKAoICAQCdLUM5mVrg6bLl6IDQ7G/yiR0b+g69kVoq3lMTVZ3EcV1xLQEABHRZfb2nqazpjZC
PztS8yceYaJQxuccZRvGicfnxxoVHK4I79TuW7iPhRMJSE7ucxFtxVioQHlQwvuIcaZkqSK8QIo7
URH5zTsav6lQnWQFsh2Q/zDL1psR8fOLDgPbX+kmYdAhapPZTRYnimlBOM6+iPWxmjTnR7zWpLat
k3dTI9Nlk+xBbWH+1sbLx8d19cvLD2aiGmaOVpV8AtNfQ/+UKurqbv7gs9WKf0mnX8nKMM6lOlqT
XNEgMHlLVeGYBkBawJzNp1nxwpxHa2tMzWPzt4Hx1C7M51LD4tKOC0rGyrnC5n5nvs8BnduF0+2
3ex57mwTBc60u1zrnVzfuZkm+42ns+P0PWGRwDE8tWNmAG2j107rqndcWtOazFsf+nYMR+Tuu
+8evyQq9egFHWM6QleMwevwwVV/Uu0tGRUHpJMKJv8KPQycZc9cGf2bg9g3L5W9fba8uzqCr6eyc
0koMcdhWFe4uHKoiGkQZ94seROWmA7K5dedU71SoxWjJVZIiJBa/LnvMJk4nK6cnm2spUj+giQLz
9I6N2jjuM8m4/onlIBP18sU131rv6sXsXYxwxzLnW98XCQWpnUi1CjASszZs01il7Nx+J3Tv pB
ocRL/bwnNQlDAQAJoBoIBBzCAYWswIfwYD7R0jBHgwfcAUQMbzgDlcQnl8IQ8Pcx/XugOzt/tkwEgYD
VR0TAQH/BAgwBgEB/wIBADBBBgNVHSAEOjA4MDYGCisGAQQBgZNoAwEwKDAmBggrBgEFBQcCARYa
aHR0cHM6Ly93d3cuYW5jZXJ0LmNvbS9jcHMwgZoGA1UdHwSBkjCBjzCBjKCBiaCBhoYqaHR0cDov
L3d3dy5hbmNlcnQuY29tL2NvbC9BTkNFUlRQVUJlVjluY3JshitodHRwOi8vd3d3Mi5hbmNlcnQu
Y29tL2NvbC9BTkNFUlRQVUJlVjluY3JshitodHRwOi8vd3d3M3y5hbmNlcnQuY29tL2NvbC9BTkNF
UlRQVUJlVjluY3JsMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUwLq6NztDegm8Wzs21rLeLfZL
fMgwJQYDVR0RBB4wHIEacGtpLmV4cGxvdGFjaW9uQGFuY2VydC5jb20wDQYJKoZIhvcNAQELBQAD
ggIBAM+LKN+ObjBPMBsS0TE2fOx2JW5WR6tuXD+eg2kFY2sG0v7hqRdCi/g9HS1iWOYhN/1jRp
DJ1RsqYR6kDVccJpQ807LV6C6G1cx7LXyUW0eFlWN7nuLSiBcGUoo9QoN4eQtK3EDg7mEpJcUre
B+YToDSaBUFK+LqQI2W9ragu8FFQ299Rf7zjkG+Z8CiIajJI9sEbUE0ExAwZAtvJhXw3CxKz8Zn
y5/e6EAE5H/Y+94Vhq4blM7EoX6xJqoYxTrzk07eVbCLLs5xFOD6RwCZWuQTcckIknSRMoFW9bSC
JnxSQUfRfv6ukNcgUi4dGUbIxs/PzTLBwu3WTDR5Vv4tb0ZRSyM7hyIGLoQjO3zpys6fvIQFWQpG
6gKU+SDwSOAOFf0NqZqLKCq3uFOHV7gP8LpUXMzIOySEu9jNwVeHstBgHTE8AbfiuDg/zHZSd9X
5Pq96bO0bPq0n4LCM08taVJojH6XHjbSqxnMU4sYEGyLR7UDCktdEx81waIqEN076XXftw02PB
mpJNxHsKE2cr0nKL+tT/1T0cMUMTJgKHc97S1hNgqaatfmHK9rWhgUfqp0AwOgv9HCvz12ETy4qS
amkwHPMCWob0ZEJb09G8rudxn7fOH6lKBw07uO2pdsYFnPeO2w+0qIE3bBGzkX5FxL92XbzWjt
iUHQ

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ANCERT Corporaciones de Derecho Publico V2*
Issuer O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Issuer C:	*ES*
Subject CN:	*ANCERT Corporaciones de Derecho Publico Personales V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*
Valid from:	*Thu May 27 10:04:55 CEST 2010*
Valid to:	*Wed May 27 10:04:56 CEST 2020*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9D:2D:43:09:E6:65:6B:83:A6:CB:97:A2:03:43:B1:BF:CA:24:74:6F:E8:3A:F6:45:68:AB:72:0C:4D:56:77:11:E5:65:C4:B4:04:00:11:D1:64:56:F6:9E:A6:B3:A6:36:42:3F:32:12:F3:27:12:61:A2:50:A2:E7:1C:65:1B:C6:89:E3:EE:C6:2A:15:1C:AE:25:EF:D4:EE:5B:B8:8F:9D:13:09:E4:4E:EE:73:11:6D:C5:58:A8:40:79:50:C2:FB:84:71:A6:64:A9:22:BC:40:8A:3B:51:11:F9:CD:3B:1A:BF:A2:10:9D:64:05:B2:1D:90:FF:30:CB:2E:9B:11:F1:F3:8B:0E:03:DB:5F:E9:26:61:D0:21:6A:93:D9:4D:16:27:8A:69:41:38:CE:BE:88:F5:B1:9A:34:E7:47:BC:D6:A4:B6:AD:93:77:53:7D:2F:65:93:EC:41:6D:61:FE:22:C6:CB:C7:C7:75:F5:CB:CB:0F:66:A2:1A:66:8E:56:95:7C:02:D3:5F:43:FF:94:2A:EA:EA:6E:FE:E0:B3:D5:8A:7C:99:A7:5F:C9:CA:30:CE:A5:3A:5A:93:5C:D1:20:30:79:4B:55:E1:98:06:40:5A:C0:9C:CD:A7:59:F1:C2:9C:47:6B:6B:4C:CD:63:F3:B7:81:E5:C7:50:AB:33:9D:4B:0F:8B:4A:38:2D:2B:1B:2A:F0:0B:99:F9:9E:FB:3C:06:77:6E:17:4F:B6:DD:EC:79:8B:B9:B0:4C:17:3A:D2:ED:73:AF:05:73:23:06:64:9B:EE:36:9E:CF:8F:38:F5:86:47:00:C4:27:CB:56:36:60:06:DA:3D:74:EE:BA:A7:75:C5:9F:39:AC:C5:B1:FF:A7:60:CF:D1:F9:3B:A2:FB:C7:AF:C9:0A:BD:7A:01:47:58:CE:90:95:E3:30:7A:FC:30:55:5F:D4:BB:4B:46:45:41:E9:24:C2:89:BF:C2:8F:43:27:19:73:D7:06:7F:66:E0:F6:0D:CB:E5:6F:5F:E9:AF:2E:CE:A0:AB:E9:EC:9C:D2:4A:0C:71:D8:56:15:EE:2E:1C:AA:22:1A:44:19:F7:8B:1E:44:E5:A6:03:B2:B9:75:E7:54:4F:54:A8:C5:68:C9:55:99:62:24:16:BF:2E:7B:CC:26:4E:27:2B:A7:27:9B:6B:29:52:3F:A0:89:02:F3:F4:8E:8D:DA:38:EE:33:C9:B8:FE:89:E5:94:13:F5:F2:C5:37:D6:BB:FA:B1:7B:17:63:1C:70:CC:B9:D6:F7:C5:C2:41:6A:62:89:4D:7F:0A:30:12:B3:36:6C:D3:58:88:EF:F3:71:F8:9D:D3:BF:FA:41:A1:E4:4B:FD:BC:27:35:02:03:01:00:01*
Authority Key Identifier	*40:C8:73:80:39:5C:42:7F:08:43:C3:DC:C7:F5:EE:80:EC:ED:FE:D9*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18920.3.1* *CPS pointer: https://www.ancert.com/cps*
CRL Distribution Points	*http://www.ancert.com/crl/ANCERTPUB_V2.crl* *http://www2.ancert.com/crl/ANCERTPUB_V2.crl* *http://www3.ancert.com/crl/ANCERTPUB_V2.crl*
Subject Key Identifier	*C0:BA:BA:37:3B:43:72:09:BC:5B:3B:36:D6:B2:DE:2D:F6:4B:7C:C8*
Subject Alternative Name	*pki.explotacion@ancert.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*26:18:A9:AC:8D:B2:5F:36:4F:DB:37:C3:9D:B3:93:AC:00:11:1A:BE:57:64:8F:EF:65:7D:75:1C:66:02:21:D2*

X509SubjectName

Subject CN:	*ANCERT Corporaciones de Derecho Publico Personales V2*

Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*
Service status description	*[en]* *undefined.*
	[es] *undefined.*
Status Starting Time	*2018-02-15T01:00:00Z*

3.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.2.2 - History instance n.1 - Status: granted

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service Name		
Name	*[es]*	*Certificados Personales de Corporaciones de Derecho Público v.2*
Name	*[en]*	*Qualified Personal Certificates for Public Corporations v2*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Corporaciones de Derecho Publico Personales V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*wLq6NztDcgm8Wzs21rLeLfZLfMg=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

3.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Personales de Corporaciones de Derecho Público v.2*
Name	*[en]*	*Qualified Personal Certificates for Public Corporations v2*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Corporaciones de Derecho Publico Personales V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*wLq6NztDcgm8Wzs21rLeLfZLfMg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-11-16T00:00:00Z*

3.3 - Service (granted): Certificados Notariales Reconocidos para personas físicas v.2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Notariales Reconocidos para personas físicas v.2*

Name *[en]* *Qualified Notarial Certificates for individuals v.2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *426856276939524068274139226323103967 63*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHvDCCBbCgAwIBAgIQIBzz7nD2CLUJvpJOScXWzANBgkqhkiG9w0BAQsFADB8MQswCQYDVQQG
EwJFUzFBMD8GA1UEChM4QWdlbmNpYSBOb3Rhcmlhbi0kZSBDZXJ0aWZpY2FjaW9uIFMuTC5VL1At
IENJRiBCODMzOTU5ODgxKjAoBgNVBAMT1UFOQ0VSVCBDZXJ0aWZpY2Fkb3MgTm90YXJpYWxlcyBW
MjAeFw0xNjA2MjEwOTUwNTlaFw0zMDA1MjUwMDAxMDBaMIHNMQswCQYDVQQGEwJFUzFEMEIGA1UE
BxM7UGFzZW8gZGVsIEdlbmVyYWwgTWFydGluZXogQ2FicG9zIDQ2IDZhIHBsYW50YSAyODAxMCBN
YWRyaWQxQTA/BgNVBAoTOEFnZWS5jaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2hvbiBTLkwuVS4g
LSBDSUYgQjgzMzk1OTg4MTUwMwYDVQQDEyxBTkNFUlQgQ2VydGlmaWNhZG9zIE5vdGFyaWFsZXMg
UGVyc29uYWxlcyBWMjCCAiIwDQYJKoZlhvcNAQEBBQADgglPADCCAgoCggIBAN9Svwb0tlsUpH+5
oOrLImObpwpKekWJKz0VOj9tudkqe4cFPUJH01J6G0pI3ojsoEHlbmsaeFwYYFzKKWsK/t6ggB1
0L6F7Adnh1TRXK7MvbFINqzGzIaynXSFRNsiGILHhqcGWsB2fyQtugsMjcJUgCqNJOc1vb77C1x
VvOKzKS5GkRf0V/+xKwQ+FRuo1Q8mL/uL+p5287YEnHp75+k8K4bHOWJarg8HzAecfdFRmYmbNZz
9cx0t73rLrBHd/UaeYk8se7hjU81qac8NZ38MBHGA/0y07iNatnG08ybfiq9cMmPS3+gy7XTUjfS
LUI3E1jALcx7xZ3KUgZB6aSpye5qY9k6NJj0Qsit1DyIK9ahBBQbzo4KCzVXtc8FRZ3MncjVTs
pRbJqq4wcJ3gFvPlPtnCKDp8Q7ty6sgB85nqHZD5vioMt8odLgXBxe1U+HYTNiK1dqLR0L4N5UJ
KAKjnc5gY0X1SA2IsCT61FP9cXtZrSDsQU7uRR7fVQHcZWvyGwOM0gwK6bt8CRsn0g5FTP3z/GQw4
x21otZo61Kw6RZJdRjAYX9wBAJu6plmqX6Tp3FK3vJ5Y0yDthfbFbgd7nPcgz7TQ2RrRq07Px7lz
srpV1YKcAPqiIZBJcRBsK0xbPMZYszySp46oxG86jrI53Ah5NsDIyKZt4vvAgMBAAGjggHyMIIB
7jCBgAYIKwYBBQUHAQEdBDBwMC8GCCsGAQUFBzABhiNodHRwOi8vb2NzcC5hYy5hbmNlcnQuY29t
L29jc3AucHVkYTA/BggrBgEFBQcwAoYzaHR0cDovL3d3dzSbbmNlcnQuY29tL3BraS92M0j9ZXJ0
cy9BTkNFUlROT1RfVjluY3J0MB8GA1UdIwQYMBaAFPYSOqt7WMGNQ292gdLyuNPvF+oLMBIGA1Ud
EwEB/wQIMAYBAf8CAQAwQQYDVR0gBDowODA2BgorBgEEAYGTaAEBMCgwJgYIKwYBBQUHAgEWGmh0
dHBzOi8vd3d3LmFuY2VydC5jb20vY3BzMIGaBgNVHR8EgZIwgYSwgYyggYmgg YaGKmh0dHA6Ly93
dXcuYW5jZXJ0LmNvbS9jcmwvQU5DRVJlTk9lNX1YyLmNybHNlYraHR0cDovL3d3dzMuYW5jZXJ0LmNvbS9jcmwvQU5DRVJU
Tk9lUX1YyLmNybDAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFG8buGSXHTz1h7oFqP/s+Oj3lNhj
MCUGA1UdEQQeMBy BGnBrzaS5leHBsb3RhY2lvbkBhbmNlcnQuY29tMA0GCSqGSIb3DQEBCwUAA4IC
AQBgfkOe1Zc4PqduiBKspDkZM42WLoXhAuHeYL5xSs9ysNoMuHMHBQPJYQX12XyUWaIzR7cn24
J0/11FJ2OoK2y7GOPcBCEO3qczHbKkYtpAR9HXQAwXcQDIbfI3v02qAPK45U2Zq08jtCvhBd8+OC
WPEx7nxWzUxIh1T00HyFox9xPoT08OtLxZXPSU+DJatQv37P3oXuUEmmWdjtVQKWiP4F5RlPzC0NY
9uD4XaRHCYp0B2CDvb/gp+ozcT32Aw4fIEcib2wAo8MBc+FR2UBS1TL686Jhn3GyE9N2SnjAiSJu
S6rK243Sc2Nsfjt6WZK+F3ITp/INBmg28CxPtu7mneL1nl/5Ecxnuvqz7kmbwzYKB+5smRQu80Zw
e6+fQv7ORwOQ4y2Z0PN9c2l2ncB/kE5rulnowP2nBxa64NbwRlDsrN27rB/+KbufzjVoHjeokv72
iYirlWDfZO1FJDCfW3iKZs1h5X1BaS6zX0TQY2LDc8QQ6aNQcX7btU/K8Rt4QTLZN9aGhgV6P62dF
ZOmDa/qmgMHm+nkyZ8BuXuZIyXOFuxCmmkasZ71cfPvuernSKHRaqG+AqTdD2LCa+gNi3rju00lv
frO3mlyeM5bBQ/770kYpvdOcW/vCJ1ybRt1ZS3Nm2LL+PRVrIoYuE9Dz1Iv9JLC8RFU2qpN9yES
vA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Certificados Notariales V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados Notariales Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Tue Jun 21 11:50:59 CEST 2016*

Valid to: *Sat May 25 02:01:00 CEST 2030*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DF:52:BF:06:F4:B4:8B:14:A4:7F:B9:A0:EA:CB:22:63:9B:A7:0A:4A:7A:45:89:2B:3D:15:3A:3F:61:B9:D9:2A:7B:87
:05:3D:42:47:D3:52:6D:1B:4A:48:DE:82:63:B2:81:07:95:B9:EC:69:E1:70:7D:81:73:90:A5:AC:2B:FB:7A:82:00:75:D0:BE:85:4C:07:67:87:54:D1:5C:AE:CC:BE:11:75:36:AC:E3:1B:32:1A:CA:75:D2:15:13:68:18:82:C7:86:
A7:86:5A:C0:7F:D9:FC:90:8A:E8:2C:32:37:B7:52:A0:AA:34:83:9C:D7:28:7B:EC:2D:71:56:F3:8A:CC:A4:B9:1A:44:5F:D1:5F:FE:C4:AC:10:F8:54:6E:A3:54:3C:98:BF:EE:2F:EA:79:DB:CE:D8:12:71:E9:EF:9F:A4:F0:AE:
1B:1C:E5:89:6A:B8:3C:1F:30:1E:72:D7:45:46:66:26:6C:D6:73:F5:CC:74:B7:BD:EB:2E:B0:47:77:F5:1A:79:89:3C:B1:EE:E1:8D:4F:35:A9:A7:3C:35:9D:FC:30:11:C6:03:FD:32:D3:B7:CD:6A:D9:C6:3B:CC:9B:7E:2A:BD:7
0:C9:8F:4B:7F:A0:CB:B5:D3:52:37:D2:2D:4D:77:13:58:C0:2D:CC:7B:C5:9D:CA:50:98:19:07:A6:92:A7:FC:9E:E6:A6:3D:93:A3:49:8E:54:2C:8A:DD:43:C8:82:BD:6A:10:41:41:BC:E8:E0:A0:B3:55:7B:3C:F0:54:59:DC:C9
:DC:8D:54:EC:A5:16:C9:AA:AE:30:70:9D:E0:16:F3:E5:3E:60:97:0E:9F:10:97:BB:72:EA:C8:01:F3:99:EA:1D:90:F9:BF:FA:0C:B7:CA:1D:2E:05:C1:FF:17:B5:53:E0:58:4C:D7:CA:D5:DA:8B:47:42:F8:37:95:09:28:02:A3:9
D:EE:60:63:45:F5:48:0D:A5:C4:24:FA:D4:53:FD:71:7B:59:AD:20:EA:41:4E:EE:45:1E:DF:55:01:DE:65:6C:A2:1B:03:8C:D2:0C:0A:EA:1F:02:46:C9:F4:83:91:53:3F:7C:FF:19:0C:38:C7:6D:68:B5:9A:3A:D4:AC:3A:45:92:
5D:46:30:18:5F:DC:01:00:9B:BA:A6:59:AA:5F:A4:E9:DC:52:B7:BC:9E:58:D3:20:ED:85:F6:C5:6E:07:7B:9C:F7:20:CF:B4:D0:D9:1A:D1:AB:4E:CF:C7:B9:73:B2:BA:55:D5:82:9C:00:FA:A2:95:90:49:71:10:6C:2B:4C:5B:
3C:C6:58:B3:3C:92:A7:8E:A8:C4:6F:3A:8E:B7:F9:DC:08:79:36:C0:C8:C8:AC:ED:E2:FF:EF:02:03:01:00:01
```


Authority Info Access

http://ocsp.ac.ancert.com/ocsp.xuda

http://www.ancert.com/pki/v2/certs/ANCERTNOT_V2.crt

Authority Key Identifier *F6:12:3A:AB:7B:58:C1:8D:43:6F:76:81:D2:F2:B8:D3:EF:17:EA:0B*

Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18920.1.1* *CPS pointer: https://www.ancert.com/cps*
CRL Distribution Points	*http://www.ancert.com/crl/ANCERTNOT_V2.crl* *http://www2.ancert.com/crl/ANCERTNOT_V2.crl* *http://www3.ancert.com/crl/ANCERTNOT_V2.crl*
Subject Key Identifier	*6F:1B:B8:64:97:1D:3C:F5:87:BA:05:A8:FF:EC:F8:E8:F7:94:D8:63*
Subject Alternative Name	*pki.explotacion@ancert.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C4:47:25:08:C3:BC:68:9F:C5:9E:8B:F7:7A:6D:DE:DF:BB:29:A4:33:16:BD:09:46:D5:44:E5:4D:FC:00:15:35*

X509SubjectName

Subject CN:	*ANCERT Certificados Notariales Personales V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.3.2 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados Notariales Reconocidos para personas físicas v.2
Name	[en]	Qualified Notarial Certificates for individuals v.2

Service digital identities

X509SubjectName

Subject CN:	ANCERT Certificados Notariales Personales V2
Subject O:	Agencia Notarial de Certificacion S.L.U. - CIF B83395988
Subject L:	Paseo del General Martinez Campos 46 6a planta 28010 Madrid
Subject C:	ES

X509SKI

X509 SK I	bxu4ZJcdPPWHugWo/+z46PeU2GM=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision
Status Starting Time	2010-11-16T00:00:00Z

3.4 - Service (granted): Certificados Notariales Reconocidos para personas jurídicas v.2

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[es]	Certificados Notariales Reconocidos para personas jurídicas v.2
Name	[en]	Qualified Notarial Certificates for legal person v.2

Service digital identities

Certificate fields details

Version:	3
Serial Number:	80355812110946286783278297140241042538

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHyjCCBbKgAwIBAgIQPHP3aufgjKEx6Z97na8MajANBgkqhkiG9w0BAQsFADB8MQswCQYDVQQG
EwJFUzFBMD8GA1UEChM4QWdlbmNpYSB3b3RhcmlhbCBkZSBDZXJ0aWZpY2FjaW9uIFMuYC5YLzAt
IENJRzBCODMzOTU5ODgxKjAoBgNVBAMTIUFOQ0VSVCBDZXJ0aWZpY2FkbXMgIm90YXJpYWxlcyBW
MjAeFw0xNjA2MjExMDA1NTZaFw0zMDA1MjUwMDAxMDBaMIHPMQswCQYDVQQGEwJFUzFEMEIGA1UE
BxM7UGFzZW8gZGVsIEdlbmVyYWwgTWFydGluZXogQ2FtcG9zIDQ2IDZhIHB5YW50YSAyODAxMCBN
YWRyaWQxQTA3BgNVBAoTOEFnZWSjaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2lvbiBTLkwuVS4g
LSBDSUYgQjgzMzk1OTg4MTcwNQYDVQQDEy5BTkNFU1lQg Q2VydGlmaWNhZG9zIE5vdGFyaWFsZXMg
Q29ycG9yYXRpdm9zIFYyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA6ckRckAGqhSM
nCwORxG/t4U0lI6VPhrk4cIBCvjA3tkDZoMGEpW3LHJQvRNOTOuyqkECUwytMLOFmQVgtgy62TN
y145lkgA/zOBrISDAHfgoEzAgTfe9JHYZYK5Et0KgeWeZAVz8SQ5K2/TmQLSxglPKYcBMuKuvtFK
FPt2C+06dLkjFbsQlbbCGUDcXIRgB+FTbBPobINXjFN9I2/8h4IB0CpP3MY8NlkZa1Bg0BGYo9q
g7is+E6x2N8PtDnlmH6/l05yDzJ1ElckMPPD8miWvJgzrs5WwrblqSoTvgfGibCmG470inLY35Q
jFBUzR7JvfE4x9kVrkPkdblj9ptd1iNaDWoGqIo6wHzfFPDtI5OgH6d83kuUctXwF6I/9ZHnJjij
IVKL9LJmFJbqcWCrlFUG+TE3T4KVNrfvz1zEm0sNS1I0wXpHVOMxX3ceOnZ8oaOq18mwAKBVxa+I
XuRtuR2sDDoDJtKDqMgIBXQN0EtKzf0bwnV8CXdI3oPvqmKfUkyHeEOoPbQzcj69Ialt9FylZcPKI
eILnJAcdC51vARu5v5nsEY4CW3SabngwEFkPwyHm9SOnrH2+HhXKSrOjeDpEHU0Xg+M7yyudWkLr
AQ062fsi0KgEw+cd6QtRaRKYcWKsXjE9E8UdKIlqV/Mb83i7qS19nI287kvgkKsCAwEAAaOCAIIw
ggHuMIGABggrBgEFBQcBAQR0MHIwLwYIKwYBBQUHMAGGI2h0dHA6Ly9vY3NwLmFuY2VydCSj
b20vb2Nzcc54dWRtbMB6CCSsGAQUFBzACbjNodHRwOi8vd3d3LmFuY2Vydc5jb20vcGlpL3YyL2N1
cnRzL0FOQ0VSVESPVF9WMi5jcnQwHwYDVR0jBBgwFoAU9hI6q3tYwY1Db3aB0vK40+8X6gswEgYD
VR0TAQH/BAgwBgEB/wIBADBBBgNVHSAEOjA4MDYGCisGAQQBgZNoAQMwKDAmBggrBgEFBQcCARYa
aHR0cHM6Ly93d3cuYW5jZXJl0LmNvbS9jcHMwgZoGA1UdHwSBkjCBjzCBjKCBiaCBhoYgaHR0cDov
L3d3dy5hbmNlcnQuY29tL2Nvb0C9BTkNFUlROT1RlVjluY3JshitodHRwOi8vd3d3Mi5hbmNlcnQu
Y29tL2Nvb0C9BTkNFUlROT1RlVjluY3JshitodHRwOi8vd3My5hbmNlcnQuY29tL2Nvb0C9BTkNF
UlROT1RlVjluY3JsMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUCKEsaDWApP+cqxFsCzOZLXEZ
qjAwJQYDVR0RBB4wHIEacGtpLmV4cGxvdGFjaW9uQGFuY2VydCSjb20wDQYJKoZIhvcNAQELBQAD
ggIBAFTAzI1a41DuQ38Qk0hUojOsnvKug4DLhug3b1NGrtQEzXhDUxDIVwPMfhCzQvbVJy/OTBC0
bETQbFfQG+92H42kTyxkHCcOsVibcyryykxnzrIDsaDFtZZe76SLKrFBv8OBQ6SvlmVS4vUWGJ
pEzGuS7dXXcTuRLCWI865YU8pbbIJYny3mdy5xA/E1UFsjIUkio7OqERkovJlLpKWWFosx7R3e3K
EORSa3Ta5ql+KycbW2cCf4yzDqLlzKUd8BY7YmSUYHsXth5qUdFKtucZLJRGTQ0AFcIrWGnH9nNx
LsIlknJE16EFc8bLiHgqZ6hxt0AcErZph7L4+Hg+rsHl0RuCokx7N5FfRJZMt6OybpPvrkcwpHOaW
omLqOPdQSIcjnJfCbZIzgpNWrHfAUScyedzKiKygJF0Tb7opp8aUbwyjKLLbOO+2ozpdM9kLdzx
f3P9jTOkih9CVWV4fQygsrv170dj82uZZIVJ87J9G73KD+OcfRcXG5tSPczrhTbt7whx5zdllZx3
e6W36ncd7g5ce1zV+575hv2zlLmVWfaFy/ZeFNdHx1yRLYr5SxlLtLolgIQEq2i6W/WYPtzZKpEA
J1MrXqbMVN6tt4j8D2smztJXQBLWuEtV09CStkprQMvfo7odFkHGhdWXpXD8d3iK8lyVAi3uYqVe
wbSm
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Certificados Notariales V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados Notariales Corporativos V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Tue Jun 21 12:05:56 CEST 2016*

Valid to: *Sat May 25 02:01:00 CEST 2030*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:E9:C9:11:72:40:06:AA:14:8C:9C:2C:0E:47:11:BF:B7:85:34:20:8E:95:3E:1A:E4:E1:C9:41:0A:F8:C0:DE:D9:03:66:83
:06:12:95:B7:2C:78:89:42:F4:4D:39:33:AE:CA:A9:04:09:4C:32:B4:C2:CE:16:64:15:82:D8:32:EB:64:CD:C8:8E:39:96:48:00:FF:33:81:AC:84:83:00:77:E0:A0:4C:C0:81:32:1E:F4:91:D8:65:82:B9:13:42:A0:79:67:99:01:5C:F
C:49:0E:4A:DB:F4:E6:40:B4:B1:82:53:CA:61:C0:4C:B8:AB:AF:B6:D1:4A:14:FB:76:0B:ED:3A:74:B9:23:15:BF:EC:42:5A:DB:08:65:03:71:77:CA:81:1F:85:4E:10:4F:A1:B9:4D:5E:31:4D:F4:8D:BF:F2:1E:08:07:40:A9:3F:
73:15:F0:D2:24:66:ED:41:83:40:46:62:8F:6A:83:B8:AC:F8:4E:B1:D8:DF:0F:B4:39:E5:98:7E:BF:97:4E:72:0F:32:49:D4:49:5C:90:C3:CF:0F:C9:A2:5A:F2:60:CE:BB:39:5B:0A:DB:96:A4:A8:4E:F8:1F:7C:68:42:98:6E:3B:D
2:29:CB:63:7E:50:8C:50:54:CD:1E:C9:BD:F1:38:C7:D9:15:AE:43:E4:75:B2:23:F6:9B:5D:D6:23:5A:0D:6A:06:A8:8A:3A:C0:7C:DF:14:F0:E2:7F:93:A0:1F:A7:7C:DE:4B:94:72:D5:F0:17:A2:3F:F5:91:E7:26:38:A3:95:52:8
B:F4:B2:66:14:96:EA:71:60:AB:94:55:06:F9:31:37:4F:82:95:36:B7:EF:CF:5C:C4:9B:4A:0D:4B:59:74:C1:7A:47:54:E3:31:5F:77:1E:3A:76:7C:A1:A3:AA:D7:C9:B0:00:A0:55:C5:AF:88:5E:E4:6E:89:1D:AC:0C:3A:03:26:D9
:03:A8:C8:08:05:74:0D:D0:47:ED:2B:3D:03:C2:65:7C:09:77:48:DE:83:EF:AA:62:89:52:4C:87:78:43:A8:3E:14:33:72:31:BD:51:A4:7D:17:29:59:70:F2:88:78:82:E7:24:07:1D:0B:9D:6F:01:1B:B9:BF:99:EC:11:8E:02:5B:74:
9A:6E:78:30:10:59:0F:C3:21:E6:F5:23:A7:AC:7D:BE:1E:15:CA:4A:B3:A3:78:3A:44:1D:4D:17:83:E3:3B:CB:2B:9D:5A:42:EB:01:0D:3A:D9:FB:22:D0:A8:04:C3:E7:1D:E9:0B:51:69:12:98:71:62:AC:5E:31:3D:13:C5:1D:28
:89:6A:57:F3:1B:F3:78:BB:A9:2D:7D:9D:FD:BC:EE:4B:E0:90:AB:02:03:01:00:01
```


Authority Info Access

http://ocsp.ac.ancert.com/ocsp.xuda

http://www.ancert.com/pki/v2/certs/ANCERTNOT_V2.crt

Authority Key Identifier *F6:12:3A:AB:7B:58:C1:8D:43:6F:76:81:D2:F2:B8:D3:EF:17:EA:0B*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.1.3

CPS pointer: https://www.ancert.com/cps

CRL Distribution Points

http://www.ancert.com/crl/ANCERTNOT_V2.crl

http://www2.ancert.com/crl/ANCERTNOT_V2.crl

http://www3.ancert.com/crl/ANCERTNOT_V2.crl

Subject Key Identifier	*08:A1:2C:68:35:80:A4:FF:9C:AB:11:6C:0B:33:99:2D:71:19:AA:30*
Subject Alternative Name	*pki.explotacion@ancert.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*0C:A8:B7:A0:15:06:CA:FA:A1:87:9E:74:91:C6:62:F8:26:4E:B3:A2:F1:F0:E0:65:7D:A3:D6:A9:12:FF:14:87*

X509SubjectName

Subject CN:	*ANCERT Certificados Notariales Corporativos V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2019-10-28T01:00:00Z*

3.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1*

3.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

3.4.4 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Notariales Reconocidos para personas jurídicas v.2

Name [en] Qualified Notarial Certificates for legal person v.2

Service digital identities

X509SubjectName

Subject CN: ANCERT Certificados Notariales Corporativos V2

Subject O: Agencia Notarial de Certificacion S.L.U. - CIF B83395988

Subject L: Paseo del General Martinez Campos 46 6a planta 28010 Madrid

Subject C: ES

X509SKI

X509 SK I CKEsaDWApP+cqxFsCzOZLXEZqjA=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

3.4.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1

3.4.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

3.4.5 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Notariales Reconocidos para personas jurídicas v.2

Name [en] Qualified Notarial Certificates for legal person v.2

Service digital identities

X509SubjectName

Subject CN: ANCERT Certificados Notariales Corporativos V2

Subject O: Agencia Notarial de Certificacion S.L.U. - CIF B83395988

Subject L: Paseo del General Martinez Campos 46 6a planta 28010 Madrid

Subject C: ES

X509SKI

X509 SK I CKEsaDWApP+cqxFsCzOZLXEZqjA=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2010-11-16T00:00:00Z

3.4.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1

3.5 - Service (granted): Certificados Reconocidos para empleados del Consejo General del Notariado v.2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Reconocidos para empleados del Consejo General del Notariado v.2*

Name *[en]* *Qualified Certificates for the Spanish Notarial Council employees v.2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *523834023247403290294157787795349659 5*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHujCCBaKgAwIBAgIQA/DeHRUTCjiVbv66WCDGEzANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFUzFBMD8GA1UEChM4QWdlbmNpYSBOb3Rhcmlhbk CBkZSBDZXJ0aWZpY2FjaW9uIFMuTC5VLiAt
IENJRzBCODMxOTU5ODgxLzAhBgNVBAMTGkFOQ0VSVCBDZXJ0aWZpY2Fkb3MgQ0dOIFYyMB4XDTE2
MDYyMTEwMjc1MloXDTMwMDUyNTAwMDEwMFowgcYxCzAJBgNVBAYTAkVTMUQwQgYDVQQHEztQYXNl
byBkZWwgR2VuZXJhbCBNYXJ0aW5leiBDYW1wb3MgNDYgNmEgcGxhbnRhIDI4MDEwIE1hZHIpZDFB
MD8GA1UEChM4QWdlbmNpYSBOb3Rhcmlhbk CBkZSBDZXJ0aWZpY2FjaW9uIFMuTC5VLiAtIENJRzBC
ODMxOTU5ODgxLjAsBgNVBAMTJUFOQ0VSVCBDZXJ0aWZpY2Fkb3MgcGFyYSBlbXBsZWFkb3MgVjfw
ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDA/8UbBs6LzMeB6oxVaFDzfQPIC6ICtlAQ
q16zsX/h0e+iRw40lyYGv2Rs9gLEFMaPOffXsppcXjArU/XJccDNMuMulHQcuFE+vniHlyVMN+F
pu51A8wJt7i4LTRFXjBvC3b2blFoZyYXm13FYUX10OJlBryK8Bzv1TB1m3AQ9qERqcop/6q6CMcr
CgFezFMgM0Wn2TRNaRMUXL3JApKQlQ5rNeKcRPfCDE7to0t2tOXFinLnpUbfjh3eaWtoKwbdHjEk
3Vz62k6KorSh3aDwyP0CfxLGK27BRXMd+J9otL4zBIIwHcmLEOykrwCwQSKVc+dyUAUGb8JdsTXW
Pz+4HTHlMss6Hfi/3GPvVc1eVe08sTGuAu9ez8NxopJlMEdFyjGeL4xtdl9fzmvQQfiH+IkS9BNw
h/zw5aSfotA1MukHs1BUd1c95nHaj9pm5OavVwTp/w6TDolqn2GGxUYNJwkAD088JjHkVMWkcsbR
+9pzuDDw1Sw68Q/tCUYvgxxIdEKxvhXCTbjUwZcbOF9HB9IzKjVgVBtXg+c+JpWzjBr1b+UPuVL
EW/4HK0bFWtsynLRCplMNFEzJ2rXNYIUXYjKJ5R+3BnTPpA3ie89cBuZ/pgeBnXMatNKdg24pv
XiUJpsTPxK37B9tqr2cMGKLiFmc24goj4Eia6JaWwIDAQABo4IB8jCCAe4wgYAGCCsGAQUFBwEB
BHQwcjAvBggrBgEFBQcwAYYjaHR0cDovL29jc3AuYWMuYW5jZXJ0LmNvbS9vY3NwLnh1ZGEwPwYI
KwYBBQUHMAKGM2h0dHAoLy93d3cuYW5jZXJ0LmNvbS9wa2kvdjIvY2VydHMvQUSDRVJUQ0dOX1Yy
LmNsdDAfBgNVHSMEGDAWgBQfbuGhmuHIt871NNlPQRQ4lCbRDASBgNVHRMBAf8ECDAGAQH/AgEA
MEEGA1UdIAQ6MDgwNgYKKwYBBAGBk2gEAjAoMCYGCCsGAQUFBwIBFhpodHRwczovL3d3dy5hbmNl
cnQuY29tL2NwczCBmgYDVR0fBIGSMIGPMIGMoIGJoIGGhipodHRwOi8vd3d3LmFuY2VydCSjb20v
Y3JsL0FOQ0VSVENHTI9WMi5jcmyGK2h0dHA6Ly93d3cyLmFuY2VydCSjb20vY3JsL0FOQ0VSVENH
TI9WMi5jcmyGK2h0dHA6Ly9kd3czLmFuY2VydCSjb20vY3JsL0FOQ0VSVENHTI9WMi5jcmwwuDgYD
VR0PAQH/BAQDAgGGMB0GA1UdDgQWBBR0mkmN2kjGgCjTSJvOV3KRKusDkzAlBgNVHREEHjAcgRpw
a2kuZXhwbG90YWNpb25AYW5jZXJ0LmNvbTANBgkqhkiG9w0BAQsFAAOCAgEAQgZJNoIKBs+sUw9Z
aTZ21bE0SY7e/W0Rkrn3J15u5cEiUk5WYrMdsB7K/SgT1LRs7G7HQLoTTkAVt+kqAF+iEx44Vc1/u
g0IoCmULl8ozcM8YnL350KeTTZtkWrrbI2ZqP2hzGgrkNKAoVFc2bleyxoYKquSxynnJUOae9rpN
hjTySGVXB0h8kkydfWG/UMhuAUzR7xbW0+tIGwT+t8AEYlbEFmXj T9kHXZEF4kL934YdhD3HQvW
im0q+GBaMmNawQAyts/LkdnOWfzUogemEszlLmltxKnlJrBspFun1BL9ve5rA4MPN1Xb7pv2pIWc
mhBIT72LhLqKjT5H5zZlU9xAMn7l/Lt7PxmbEZ+IW6d683h14W4zOQTA221Rhkl6DsDdoE25tqq
iW/9KnrDtI3GjZoIpIZuqXSIaH7mgSinrLkzNqQYxvJ+qqdO3jodTOlI1/mujJeMnb2xGxtd9
IyCCg0H0/z7VLIL8T/NJH4DvUxT13WhEkJg91yCHzIBw1HessyEXRRGDbgJFz4aotHmHGgvjbQA
JyoZd4gRbKG7DsjAEjDR4ubmCbwb2YFuErfl5CAfGBZJXKcQjcpC1NJNjm5bE/ZUcx57WMDr6G8
JTwYptsn1lSwV1F0qd6I16iFmm0CN8KQeuP2x+i+WDLzYZpYyOg5DPCCvUU=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Certificados CGN V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados para empleados V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Tue Jun 21 12:27:52 CEST 2016*

Valid to: *Sat May 25 02:01:00 CEST 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C0:FF:C5:1B:06:CE:8B:CC:C7:81:EA:8C:55:B8:50:F3:7D:03:C8:0B:A2:02:B6:50:10:AB:5E:B3:B1:7F:E1:D1:EF:A2:47:0E:34:97:26:06:BF:64:6C:F6:02:C4:14:C6:8F:39:F7:ED:5E:CA:69:71:78:C0:AD:4F:D7:25:C7:03:34:CB:8C:BA:51:D0:72:E1:44:FA:F9:E2:1E:5C:95:30:DF:85:A6:EE:75:03:CC:09:B7:B8:B8:2D:34:45:5E:30:6F:0B:78:76:6E:51:68:67:26:17:98:8D:C5:61:45:F5:D0:E2:65:06:2C:8A:F0:1C:EF:D5:30:75:9B:70:10:F6:A1:11:A9:CA:29:FF:AA:BA:08:C7:2B:0A:01:1E:CC:53:20:33:45:A7:D9:34:4D:69:13:14:5C:BD:C9:02:92:90:95:0E:6B:35:E2:9C:44:F7:C2:0C:4E:EB:A3:4B:76:B4:E5:C5:9C:B9:E9:51:B7:EB:8E:1D:DE:69:6B:68:2B:06:DD:1E:31:24:DD:5C:FA:DA:4E:8A:A2:B4:A1:DD:A0:F0:C8:FD:02:7F:12:C6:2B:6E:C1:45:73:1D:F8:9F:68:B4:BE:33:04:8B:70:1D:C9:8B:10:EC:A4:9F:00:B0:41:22:95:7B:E7:72:50:05:06:87:C2:5D:B1:35:D6:3F:3F:B8:1D:31:E5:32:CB:3A:1D:FB:3F:DC:63:EF:55:CD:5E:55:ED:3C:B1:31:AE:02:EF:5E:CF:C3:71:A2:92:65:30:47:45:CA:31:9E:2F:8C:6D:76:5F:5F:CE:7B:D0:41:F8:87:F8:89:12:F4:13:70:87:FC:F0:E5:A4:9F:A2:D0:35:32:E9:07:B3:50:54:77:57:3D:E6:71:DA:8F:DA:66:E4:E6:AF:57:04:E9:FF:0E:93:0E:89:6A:9F:61:86:C5:46:0D:23:09:00:0F:4F:3C:26:31:E4:54:C5:A4:72:C6:D1:FB:DA:73:B8:30:F0:D5:2C:3A:F1:0F:ED:09:46:2F:83:1C:5F:74:42:B1:BE:15:C2:4D:B8:D4:C1:97:1B:38:5F:47:07:D2:73:2A:35:60:54:1B:57:83:E7:3E:26:95:B3:8D:F0:62:D5:BF:94:3E:E5:4B:11:6F:F8:1C:A3:A1:15:6B:6C:CA:72:D1:0A:92:0C:34:51:33:27:6A:E2:5C:D6:25:52:55:D8:8C:A2:79:47:ED:C1:9D:33:E9:03:78:DE:F3:D7:01:B9:9D:69:81:E0:67:5C:C6:9F:34:A7:60:DB:8A:6F:5E:25:14:A6:C4:CF:C4:AD:FB:07:DB:6A:AF:67:0C:18:A2:E2:16:67:36:E2:0A:23:03:81:22:6B:A2:5A:5B:02:03:01:00:01

Authority Info Access

http://ocsp.ac.ancert.com/ocsp.xuda

http://www.ancert.com/pki/v2/certs/ANCERTCGN_V2.crt

Authority Key Identifier *05:6E:E1:A1:9A:EE:07:AF:CE:F5:B4:D3:65:3D:04:50:E2:D0:9B:44*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.4.2

CPS pointer: https://www.ancert.com/cps

CRL Distribution Points

http://www.ancert.com/crl/ANCERTCGN_V2.crl

http://www2.ancert.com/crl/ANCERTCGN_V2.crl

http://www3.ancert.com/crl/ANCERTCGN_V2.crl

Subject Key Identifier *74:9A:49:8D:DA:48:C6:80:28:D3:48:9B:CE:57:72:91:2A:EB:03:93*

Subject Alternative Name *pki.explotacion@ancert.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E7:18:F6:7C:8B:1F:8E:1F:C0:17:6A:36:1C:98:E6:29:9F:D3:F4:39:CF:A4:6E:DD:B4:6A:57:B4:AC:08:B4:43*

X509SubjectName

Subject CN: *ANCERT Certificados para empleados V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2019-08-08T00:00:00Z

3.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.5.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.4.2.1.3.1*
Description		

3.5.3 - History instance n.1 - Status: granted

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos para empleados del Consejo General del Notariado v.2*
Name	*[en]*	*Qualified Certificates for the Spanish Notarial Council employees v.2*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados para empleados V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*dJpJjdpIxoAo00ibzldykSrrA5M=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

3.5.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.5.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos para empleados del Consejo General del Notariado v.2*
Name	*[en]*	*Qualified Certificates for the Spanish Notarial Council employees v.2*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados para empleados V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*dJpJjdpIxoAo00ibzldykSrrA5M=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-11-16T00:00:00Z*

3.6 - Service (granted): Certificados Reconocidos de Notario v.2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Reconocidos de Notario v.2*

Name *[en]* *Spanish Notaries Qualified Certificates v.2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *572114865009836210360461163534503358 24*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHsDCCBZigAwIBAgIQKwqIEHu459XN94rCrO5cUDANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFUzFBMD8GA1UEChM4QWdlbmNpYSBOb3Rhcmlhbi5BZSBDZXJ0aWZpY2FjaW9uIFMuTC5VLiAt
IENJRiBCODMzOTU5ODgxIzAhBgNVBAMTGkFOQ0VSVCBDZXJ0aWZpY2Fkb3MgQ0dOIFYyMB4XDTE2
MDYyMTEwMjQ1MVoXDTMwMDUyNTAwMDEwMFowgbwxCzAJBgNVBAYTAkVTMUQwQgYDVQQHEztQYXNl
byBkZWwgR2VuZXJhbCBNYXJ0aWSIoBDYW1wb3MgNDYgNmEgcGxhbnRhIDI4MDEwIEIhZFIJpZDFB
MD8GA1UECbM4QWdlbmNpYSBOb3Rhcmlhbi5BZSBDZXJ0aWZpY2FjaW9uIFMuTC5VLiAtIENJRiBC
ODMzOTU5ODgxJDAiBgNVBAMTG0FOQ0VSVCBDZXJ0aWZpY2Fkb3MgRkVSTiBWMjCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAKK4EokkheZKjy5uTxqIUkyq0+GD2DeboIU0NlTyqa+JeTd
xWu2weCQ3atBBrE+VVPKG2t7HjkT8YYu2uPmKzkwQNcI8yRJolSWFOqGDaWltVis8RtrRrzbSk45
jpcM0j2ceY8nSyiGimG8Fg7AzDao4EHB9DYRjrdgtO61vUvgzc3rpp2tDkxve94EinOMFgsnONEz
r9WSdC2dhiR+YmmCMFS/MSmAHOFBm9f4fWcuP1f4PAhbAuKDiPKZKtT3A+td8VxEvYIKX3OHADY
30FsJIbfvhYBetu0sE+j+MOo097848dwd4qxC2ZYk2H7gYJL1AXO10poOjX/7yw8wRyd9/9EU+f9
vgfFJt8s8TP9ZvwJbhj5Uae+oPDUDRg0/8T6Lcds1ELZoeNr/YCzGMkem8CqWk5uBAD0D5rx/I2
qN+LSVewYoNEAm+Zgu72sbCHPb0l2QadlOrWaqJotleH8+o/6zKKPOUnJbxZ5eqsV/IHjFNA8x7r
hABqy1PCr3lGxslbJ13+MXjqMHoeZow/93Zr/0EcxzQ7WQRKtxOIqxan7bRvATprKIH0NrXNyche
wJTjZWIYrzJb9qD24/blZwpS/sqLiOp+0L35vDeFGvHPWUzKC+uQuMBJkokEIupHSW1NvqGnsFgH
b+SGCkLK2mHz T0ZdVudiZsCsf4lDAgMBAAGjggHyMIIB7jCBgAYIKwYBBQUHAQEEdDByMC8GCCsG
AQUFBzABhINodHRw Oi8vb2NzcC5hYy5hbmNlcnQuY29tL3Bra592M6ZXJ0cy9BTkNFUlRDR05fVjIuY3J0MBBGA1Ud
IwQYMBaAFAVu4aGa7gevzvW002U9BFDi0JtEMBIGA1UdEwEB/wQIMAYBAf8CAQAwQQYDVR0gBDow
ODA2BgorBgEEAYGTaAQBMCgwJgYIKwYBBQUHAgEWGmh0dHBzOi8vd3d3LmFuY2VydC5jb20vY3Bz
MIGaBgNVHR8EgZIwgY8wgYyggYmggYaGKmh0dHA6Ly93d3cuYW5jZXJ0LmNvbS9cmwvQU5DRVJU
Q0dOX1YyLmNvbIYraHR0cDovL3d3dzIuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ0dOX1YyLmNybIYr
aHR0cDovL3d3dzMuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ0dOX1YyLmNybDAOBgNVHQ8BAf8EBAMC
AYYwHQYDVR0OBBYEFF+TQLU4CCTO8L8jTrkvIRNoroT7MCUGA1UdEQQeMByBGnBraS5leHBsb3Rh
Y2lvbkBhbmNlcnQuY29tMA0GCSqGSIb3DQEBCwUAA4ICAQAZa7iY7K3V52eL13pOvKE629W+eW7k
oKkNM5JB11XJbFitBSr7tZ5YqOkoKQpW9b9hzuzEL4DbbMzctny8IWHBLevA1rKteNpvXkBKqWs
VfK/lSkvgr2sEozqcCTQKhL27VnsQ71tKY725k6TM8vAmPhEqmy++4vnHiKIEg07nkjLA73Zulcb
3geF93ErSNCfjdwpmYhLA6l7e+UozgJldx0HQC4CGzXalezlVaRzQuzAr8OY9fNr4qJhrF1qMYhv
AQX0gumNNlchABXWLJxsXcIHtSCDYgTL/K8cm4BLW+pjD63tcSTkXB0b1EYzi6rPvcOC5L6EmT/k
SdC9+tIE3pGcXjBYLWjUECoirvL8oQAHuTIGwQDCcec+Fe9XfISu44JLSeLOgr1rzNRSnL+IGibO
XnuPUY/lH9knXU1IyEg4uBKgxe4Ced2wKdavBepkonq+T3c5hUW5I3W3PXYOTPYJI3TXW0Cq4h0j
qednmooj1pior3CkFBYHvumtQvYcjHAiaGcGnAj/J8V/yp8Vl4vXZ9cZMmHwOQX8/V3xfGQ5itV4
gQSobnaYfDmesyJ3625AH1e53Xnilsu5MWStLpDdcnFYNo2QGvc5DzWCUn3f+sx+Jwy+NTHIHJvt9
2wRx6cHGdavn/ZuvORrMx3K2s1cLjVKxq4F31rZCuZ+UJw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Certificados CGN V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados FERN V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Tue Jun 21 12:24:51 CEST 2016*

Valid to: *Sat May 25 02:01:00 CEST 2030*

Public Key:

```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A2:B8:12:89:24:85:E6:4A:8F:2E:6E:4F:1A:9F:52:4C:AA:D3:E1:83:D8:37:9B:A0:85:2D:D0:D9:53:CA:A6:BE:25:E4:
DD:C5:6B:B6:C1:E0:90:DD:AB:41:06:B1:3E:55:53:CA:1B:6B:7B:1E:39:13:F1:86:2E:DA:E3:E6:2A:B9:30:40:D7:08:F3:24:49:A2:54:96:14:EA:86:0D:A5:88:B5:58:A2:F1:1B:6B:46:BC:DB:4A:4E:39:8E:97:8C:D2:3D:A8:7
9:8F:27:B1:2F:E3:1A:29:C6:F0:48:3B:03:30:DA:A3:81:07:07:D0:D8:46:3A:F8:82:03:BA:D6:F5:2F:83:37:37:CE:9A:76:7C:39:31:BD:EF:78:12:73:B8:16:AB:27:38:D1:33:AF:D5:92:74:2C:DD:86:24:7E:62:79:82:30:54:BF:3
1:29:80:1C:E1:41:9B:D7:F8:7D:67:2E:3F:57:F8:3C:08:5B:02:E2:9F:26:23:CA:64:AB:53:DC:0F:AD:77:C5:71:12:F6:08:29:7D:CE:1C:00:D8:DF:41:6C:24:86:DF:BE:16:01:7A:DB:B4:B0:4F:A3:F8:C3:A8:D3:DE:FC:E3:C7:
70:77:8A:B1:0B:66:58:93:61:FB:81:82:4B:94:05:CE:D7:4A:68:42:35:FF:EF:2C:3C:C1:1C:9D:F7:FF:44:53:E7:FD:BE:07:C5:26:DF:2C:F1:33:FD:66:FC:09:6E:18:F9:51:A7:BE:A0:F0:D4:0D:18:34:FF:C4:FA:2D:E7:6C:24:4
2:D9:A1:C3:6B:FD:80:B3:18:C9:1E:9B:C0:AA:5A:4E:6E:04:00:F4:0F:9A:F1:FC:87:F6:A8:DF:8B:49:57:B0:62:83:44:02:6F:99:82:EE:F6:B1:B0:87:3F:A7:CB:D9:06:9D:20:EA:D6:6A:A2:33:D1:E1:FC:FA:8F:FA:CC:A2:8F
:39:49:C9:87:16:79:FD:EA:AC:57:F2:07:8C:53:40:F3:1E:EB:84:00:6A:CB:53:C2:AF:72:06:C6:C9:5B:27:5D:FE:31:78:EA:30:7A:1E:66:8C:3F:F7:76:6B:FF:41:1C:C7:34:3B:59:04:4A:B7:13:88:AB:16:A7:ED:B4:6F:01:3A:6
B:28:81:F4:36:B5:CD:C9:C8:5E:C0:94:E3:65:62:18:AF:32:5B:F6:A0:F6:E3:F6:C8:67:0A:52:FE:CA:8B:88:EA:7E:D0:BD:F9:BC:37:85:1A:F1:CF:59:4C:CA:0B:EB:90:B8:C0:49:92:89:04:22:EA:47:49:6D:4D:BE:A1:A7:B0:
58:07:6F:E4:86:0A:42:CA:DA:61:F3:4F:46:5D:56:E7:62:66:C0:AC:7F:89:43:02:03:01:00:01
```

Authority Info Access *http://ocsp.ac.ancert.com/ocsp.xuda*

http://www.ancert.com/pki/v2/certs/ANCERTCGN_V2.crt

Authority Key Identifier *05:6E:E1:A1:9A:EE:07:AF:CE:F5:B4:D3:65:3D:04:50:E2:D0:9B:44*

Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18920.4.1* *CPS pointer: https://www.ancert.com/cps*
CRL Distribution Points	*http://www.ancert.com/crl/ANCERTCGN_V2.crl* *http://www2.ancert.com/crl/ANCERTCGN_V2.crl* *http://www3.ancert.com/crl/ANCERTCGN_V2.crl*
Subject Key Identifier	*5F:93:40:B5:38:08:24:CE:F0:BF:23:4E:B9:2F:95:13:68:AE:84:FB*
Subject Alternative Name	*pki.explotacion@ancert.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*A8:85:EC:82:18:B1:C9:67:30:B0:26:4E:CF:BB:DE:E0:6C:97:B7:01:FA:F8:0D:CC:B2:69:20:F5:E7:27:AD:73*

X509SubjectName

Subject CN:	*ANCERT Certificados FERN V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-08-08T00:00:00Z

3.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.6.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.4.1.1.3.1*
Description		

3.6.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos de Notario v.2*
Name	*[en]*	*Spanish Notaries Qualified Certificates v.2*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados FERN V2*
Subject O:	*Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*X5NAtTgIJM7wvyNOuS+VE2iuhPs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

3.6.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.6.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[es]	Certificados Reconocidos de Notario v.2
Name	[en]	Spanish Notaries Qualified Certificates v.2

Service digital identities

X509SubjectName

Subject CN:	ANCERT Certificados FERN V2
Subject O:	Agencia Notarial de Certificacion S.L.U. - CIF B83395988
Subject L:	Paseo del General Martinez Campos 46 6a planta 28010 Madrid
Subject C:	ES

X509SKI

X509 SK I	X5NAtTgIJM7wvyNOuS+VE2iuhPs=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision
Status Starting Time	2010-11-16T00:00:00Z

3.7 - Service (withdrawn): Certificados Notariales Reconocidos para personas físicas

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[es]	Certificados Notariales Reconocidos para personas físicas
Name	[en]	Qualified Notarial Certificates for individuals

Service digital identities

Certificate fields details

Version:	3
Serial Number:	222481592478305966459721756209740642910

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGJzCCBQ+gAwIBAgIRAKdgZWb/yQvcOlCahER+I4wDQYJKoZIhvcNAQEFBQAwgYMxCzAJBgNV
BAYTAkVTMUswSQYDVQQKE0JBZ2VuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlpYWNpb24gUy5MLiBV
bmlwZXJzb25hbCAtIENJRiBCODMzOTU5ODgxIzAlBgNVBAMTHkFOQ0VSVCBDZXJ0aWZpY2Fkb3Mg
Tm90YXJpYWxlczAeFw0wNDAyMTIxMjI5MDdaFw0xNDAyMTIxMjI5MDVaMIHYMQswCQYDVQQGEwJF
UzEPMA0GA1UECBMGTWFkcmlkMTcwNQYDVQQHEy5QYXNlbyBkZWwgR2VuZXJhbCBNYXJ0aWS1eiBD
YW1wb3MgNDYiNmEgcGxhbnRhMUswSQYDVQQKE0lBZ2VuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlp
YWNpb24gUy5MLiBVbmlwZXJzb25hbCAtIENJRiBCODMzOTU5ODgxMjAwBgNVBAMTKUFOQ0VSVCBD
ZXJ0aWZpY2Fkb3MgTm90YXJpYWxlcyBQZXJzb25hbGVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA3nVeBMU/bnlGq/9Zy30k46DjiWT7fS5AsADK92OyYSs+AOlpSlijYLck5F2acp2T
4uPRdHDYiS98Sd6GU37UP+kD3xJX/FmPloQbSgonybVTcPrtPatOiikUczOZqJGYhhY3WLTMo7x
70BzdI0Y0IU/3GX+eoQ9wzfYYrc9c7qBp69H4je+ec8Ck89gzA0kxD6uTbWQtnnncYFIYvXmjmzI8
BFDxGIM1IeincPDVZSIlY7hMZr/PFOyMQzmLmB3+02cupHL+RpAZmN9gCpEtPwaJIDR43cIoGJKc
OQCjjmTm9tZusYPSSJT5i3yeYGayCjmxRj5ePI5ReTIY6I+LiQIDAQABo4ICPTCCAjkwHwYDVR0j
BBgwFoAUhPf8cl6IZGYdKJywd70Map9MTWIwEgYDVR0TAQH/BAgwBgEB/wIBADCCASEGA1UdIASC
ARgwggFUMIIBEAYKKwYBBAGBK2gBATCCAQAwJQYIKwYBBQUHAgEWGWhttdHA6Ly93d3cuYWSjZXJ0
LmNvbS9jcHMwgdYGCCsGAQUFBwICMIHJMA0WBkFOQ0VSVDADAgEBGoG3QWdlbmNpYSBOb3Rhcmlh
bCBkZSBDZXJ0aWZpY2FjaW9uLiBMYSBkZWNsYXJhY2lvbiBkZSBwcmFjdGljYXMgZGUgY2VydGlm
aWFjaW9uIHF1ZSByaWdlIGVsIGZ1bmNpb25hbWllbnRyIGRlIGxhIHByZXNlbnRlIGFldG9yaWRh
ZCBzZSBlbmN1ZW50cmEgZGlzcG9uaWJsZSBlbBodHRwOi8vd3d3LmFuY2VydC5jb20vY3BzMIGP
BgNVHR8EgYcwgYQwgYGgf6B9hidodHRwOi8vd3d3LmFuY2VydC5jb20vY3JsL0FOQ0VSVE5PVC5j
cmyGKGh0dHA6Ly93d3cyLmFuY2VydC5jb20vY3JsL0FOQ0VSVE5PVC5jcmywwDgYDVR0PAQH/BAQDAgGMBwGA1UdEQQVMBOB
EWFuY2VydE8bbmNlcnQuY29tMB0GA1UdDgQWBBSIEn+3Q9tRKWfGdpXq79njdcXBNTANBgkqhkiG
9w0BAQUFAAOCAQEAAIZPE33Umc6sNG3CQ0aRSmMuMU/xe1f9jKP5OCk7fSXZ5IkfkzYc1QDcY9/b
YRg9z1lh5kml7phIZtExPTjyJ4C04/qFo2+NdKFrJuKapjy+JN2SxeyeoNSAmqtN+Hw9wGfjQ5Uv
acgzyTnMdpFXVnQsA0vlEapAHeF/EvbbDQIIDGttIFGCz23aZ3R32zdN6Em4GEBv8ZHcdHfamG
NbTN8aFRyuzn5UTVMyzOKEoKeT5yxIMthRAvQho2cKYIot9vGjwVnqttPAoff2lX5iGI1eWKsuh
nYILIa/x95Rzv7Ia1hET4jLwgz48bM+aJYpPvA7umA9NY2ok1k7qIA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ANCERT Certificados Notariales*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados Notariales Personales*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Valid from: *Thu Feb 12 13:29:07 CET 2004*

Valid to: *Wed Feb 12 13:29:05 CET 2014*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DE:75:5E:04:C5:1B:9C:81:AA:FF:D6:72:DF:49:38:E8:38:A3:59:3E:DF:4B:90:2C:00:32:BD:D8:2B:72:61:2B:3E:00:
E9:69:48:88:A3:60:B7:24:E4:5D:9A:72:9D:93:E2:E3:D1:74:70:D8:89:2F:7C:E5:DE:86:53:7E:D4:3F:E9:03:DF:12:57:FC:59:8F:96:84:1B:4A:0A:27:C9:B5:53:70:FA:ED:3D:AB:4E:8A:29:14:7B:3D:19:8E:A2:06:62:18:58:D
D:62:D3:32:8E:F1:EF:40:73:E0:8D:18:D0:85:3F:DC:65:FE:7A:84:3D:C3:37:D8:62:B7:BD:73:BA:81:A7:AF:47:E2:3A:3E:7B:C0:A4:F3:D8:33:03:49:2F:0F:AB:93:6E:25:90:9E:79:DC:60:52:18:AD:79:A3:9B:32:3C:04:50:F
1:18:83:35:21:E8:A7:70:F0:D5:65:27:C9:63:B8:4C:66:BF:CF:14:EC:8C:43:39:8B:98:1D:FE:D3:67:2E:A4:72:FE:46:90:19:98:DF:60:0A:91:2D:3F:06:89:20:34:78:DD:C2:28:18:92:9C:39:00:A3:8E:64:E6:F6:D6:6E:B1:83:D2:
48:94:F9:8B:7C:9E:60:66:B2:0A:39:F1:46:3E:5E:3C:8E:51:79:37:D8:E8:8F:8B:89:02:03:01:00:01
```


Authority Key Identifier *84:F7:FA:72:5E:88:64:66:1D:28:8C:B0:77:BD:0C:6A:9F:4C:4D:62*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.1.1

CPS pointer: http://www.ancert.com/cps

CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en http://www.ancert.com/cps]

CRL Distribution Points

http://www.ancert.com/crl/ANCERTNOT.crl

http://www2.ancert.com/crl/ANCERTNOT.crl

http://www3.ancert.com/crl/ANCERTNOT.crl

Subject Alternative Name *ancert@ancert.com*

Subject Key Identifier *A5:12:7F:B7:43:DB:51:29:67:C6:76:95:EA:EF:D9:E3:75:C5:C1:35*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D7:90:51:96:05:C9:5A:B0:01:18:BD:98:62:29:0A:E9:AF:02:47:3F:22:33:76:B8:EA:33:D3:1A:60:FE:9F:C5*

X509SubjectName

Subject CN: *ANCERT Certificados Notariales Personales*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

3.7.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.1.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.1.2.1*

3.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.7.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Notariales Reconocidos para personas fisicas*
Name	*[en]*	*Qualified Notarial Certificates for individuals*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados Notariales Personales*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*pRJ/t0PbUSlnxnaV6u/Z43XFwTU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-03-09T23:00:00Z*

3.7.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.1.1.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.1.1.2.1*

3.7.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Notariales Reconocidos para personas fisicas*
Name	*[en]*	*Qualified Notarial Certificates for individuals*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados Notariales Personales*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*pRJ/t0PbUSlnxnaV6u/Z43XFwTU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

3.7.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.1.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.1.2.1*

3.8 - Service (withdrawn): Qualified Notarial Certificates for legal person

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Notarial Certificates for legal person*

Name *[es]* *Certificados Notariales Reconocidos para personas jurídicas*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *212003062634088765728504395040296052458*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGKTCCBRGgAwIBAgIRAJ9+Ti5i73AmyF1Ra5PQpuowDQYJKoZIhvcNAQEFBQAwgYMxCzAJBgNV
BAYTAkVTMUswSQYDVQQKE0JBZVuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlj YWNpb24gUy5MLiBV
bmlwZXJzb25bbCAtIENJRiBCODMzOTU5ODgxJzAlBgNVBAMTHkFOQ0VSVCBDZXJ0aWZpY2Fkb3Mg
Tm90YXJpYWxlczAeFw0xMTAyMjIxMDM0NDJaFw0yMTAyMjIxMDM0NDNaMIHaMQswCQYDVQQGEwJF
UzEPMA0GA1UECBMGTWFkcmlkMTcwNQYDVQQHEy5QYXNlbyBkZWwgR2VuZXJhbCBNYXJ0aW5leiBD
YW1wb3MgNDYtNmFzgGxhbnRhMUswSQYDVQQKE0JBZVuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlj
YWNpb24gUy5MLiBVbmlwZXJzb25bbCAtIENJRiBCODMzOTU5ODgxNDAyBgNVBAMTK0FOQ0VSVCBD
ZXJ0aWZpY2Fkb3MgTm90YXJpYWxlcyBDb3Jwb3JhdGl2b3MwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCsZI1GstoZS20nyehRss8jFsaPdyK9ef3+Iw67TxjguCh7q+PEJWG4I0E YCDu
U9DnAzFsczHojiTVcuDH9NldDLzuwHoWF3iqAaAN5Ec1300PmIEP3Sgx0XXEjEj1D1KrpqMCJj
1NKb/Gpl8ehzCz HK0fIA0Asp9GHprSQQIH1yACd6T6JID+SUUn8Wr0hO25u7fj8iRVJwBq0j2Sj
A0I3iqQxA0h97/Y1GYMPJGV7+os+nW7jHJ4sk7N5fT1FPb/FO+LL0RfG8odH401UxweSLhUFbuls
iN6oKCVP3McRmkXtN1b9l5wByLHpy4dG7Cdy TgTxbC2bOJrG3rVZAgMBAAGjggI9MIICOTAfBgNV
HSMEGDAWgBSE9/pyXohkZb0ojLB3vQxqn0xNYjASBgNVHRMBAf8ECDAGAQH/AgEAMIIBIQYDVR0g
BIIBGDCCARQwggEQBgorBgEEAYGTaAEDMIIBADAIBggrBgEFBQcCARYZaHR0cDovL3d3dy5hbmNl
cnQuY29tL2NwczCB1gYIKwYBBQUHAgIwgckwDRYGQU5DRVJUMAMCAQEagbdBZ VuY2lhIE5vdGFy
aWFsIGRlIENlcnRpZmlj YWNpb24uIExhIGRlY2xhcmFjaW9uIGRlIHByYWN0aWNhcyBkZSBjZXJ0
aWZpYWNpb24gcXVlIHJpZ2UgZWwgZnVuY2lvbmFtaWVudG8gZGUgbGEgcHJlc2VudGUgYXV0b3Jp
ZGFkIHNlIGVuY3VlbnRy YSBkaXNwb25ibYmxlIGVuIGlhIdHA6Ly93d3cuYW5jZXJ0LmNvbS9jcHMw
gY8GA1UdHwSBhzCBhDCBgaB/oH2GJ2h0dHA6Ly93d3cuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUTk9U
LmNybIYoaHR0cDovL3d3dzIuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUTk9ULmNvbIYoaHR0cDovL3d3
dzMuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUTk9ULmNybDAOBgNVHQ8BAf8EBAMCAYYwHAYDVR0RBBUw
E4ERYW5jZXJ0QGFuY2Vyd C5jb20wHQYDVR0OBBYEFFEaK24vzkos4XnQHlHuJDddE4yrMA0GCSqG
SIb3DQEBBQUAA4IBAQA19RcLx00Cgb7Anf6A7mVcd8N+FDvApMuzADpC2EfgmMTKT+SewbS13KZp
KjaZrpvRY2Q b0GtpOGC4aqvIeZLfclBGitNuAX84BLWrkiNzg2KWDom5iqQBgIXUz6tT0mlOGz4y
I3/kWq+aeKah6RYLxxVqdU6w/Qzl5qcjbrIdCVbvFvTjXqGrj3UAHhZDK2aLXa7cs8lSgXS00oeSU /
BTiZ+YSWZVAzQWmK/zIbumb4RIzXCXMaHnLMIdeunEbYbZ/URCY/KRKK5NyDkO8K5V9Vp7a6ztOCI
K9WNpYdqNWGd9ecPBLr9pHelqCk0DCXH5ITUEpW2WkP+9MTCgUaVddd B

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *ANCERT Certificados Notariales*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados Notariales Corporativos*

Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*
Valid from:	*Tue Feb 22 11:34:42 CET 2011*
Valid to:	*Mon Feb 22 11:34:43 CET 2021*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:66:5D:46:B2:DA:19:4B:6D:27:C9:E8:51:8A:CB:3C:8C:5B:1A:3D:DC:8A:F5:E7:C9:FA:5C:3A:ED:3C:63:82:E0:A1:EE:AF:8F:12:55:86:E0:8D:04:60:20:EE:53:D0:E7:03:31:6C:73:31:E8:8E:34:D5:72:E0:C7:F4:D9:5D:0C:BC:EE:C0:7A:16:17:7B:80:68:03:79:11:CD:77:D3:43:E6:20:42:0F:DD:28:31:F5:75:D7:12:31:23:D4:3D:75:2A:BA:6A:30:22:63:D4:D2:9B:FC:6A:65:F3:86:F3:0B:3F:C7:2B:47:C8:03:40:2C:A7:D1:87:A6:B4:90:42:51:F5:C8:00:9D:E9:3E:89:20:3F:92:51:49:FC:5A:BD:1A:3B:6E:6E:ED:F8:FC:89:15:49:C0:1A:B4:8F:64:A3:03:42:37:8A:A4:31:03:48:7D:EF:F6:35:19:83:0F:24:65:7B:FA:8B:3E:9D:6E:E3:1C:9E:31:93:B3:79:7D:3D:45:3E:1F:C5:3B:E2:CB:D1:17:C6:F2:87:47:E3:4D:54:C7:07:92:2E:15:05:6E:E9:6C:88:DE:A8:28:25:4F:DC:C7:11:9A:45:ED:37:56:FD:97:9C:01:C8:B1:E9:CB:87:46:EC:27:72:4E:04:F1:6C:2C:DB:38:9A:C6:DE:B5:59:02:03:01:00:01*
Authority Key Identifier	*84:F7:FA:72:5E:88:64:66:1D:28:8C:B0:77:BD:0C:6A:9F:4C:4D:62*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18920.1.3* *CPS pointer: http://www.ancert.com/cps* *CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en http://www.ancert.com/cps]*
CRL Distribution Points	*http://www.ancert.com/crl/ANCERTNOT.crl* *http://www2.ancert.com/crl/ANCERTNOT.crl* *http://www3.ancert.com/crl/ANCERTNOT.crl*
Subject Alternative Name	*ancert@ancert.com*
Subject Key Identifier	*51:1A:2B:6E:2F:CE:4A:38:5E:74:08:B6:51:EE:8C:37:5D:13:8C:AD*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*39:35:94:82:D2:AE:7D:F8:48:A1:E5:6D:E1:84:EB:9B:FA:B9:D9:83:09:C3:CD:2E:D0:97:A1:8C:BE:07:F2:40*

Certificate fields details

Version:	*3*
Serial Number:	*126356436681186619492921660190540379841*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGKDCCBRCgAwIBAgIQXw9dUFVJzZ1IdtEvb9c2wTANBgkqhkiG9w0BAQUFADCBgzELMAkGA1UE
BhMCRVMxSzBJBgNVBAsTQkFnZW5jaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2lvbiBTLkwuIFVu
aXBlcnNvbmFsIC0gQ0IGIE4MzM5NTk4ODEnMCUGA1UEAxMeQU5DRVUlIENlcnRpZmlYWRvcyBO
b3RhcmlhbGVzMB4XDTA0MDIxMjEzMDAyMFoXDTE0MDIxMjEzMDAxMlowgdoxCzAJBgNVBAYTAkVT
MQ8wDQYDVQQIEwZNYWRyaWQxNzA1BgNVBAcTLlBhc2VvIGRlbCBHZW5lcmFsIE1hcnRpbmV6IENh
bXBvcyA0Ni02YSBwbGFudGExSzBJBgNVBAoTQkFnZW5jaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNh
Y2lvbiBTLkwuIFVuaXBlcnNvbmFsIC0gQ0IGIE4MzM5NTk4ODE0MDIGA1UEAxMrQU5DRVUlIENl
cnRpZmlYWRvcyBOb3RhcmlhbGVzIENvcnBvcmFtaXZvczCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKxmXUay2hlLbSI26FGKyzyMWxo93Ir158n6XDrtPGOC4KHur48SVYbgQRgIO5T
0OcDMWxzMeiONNVy4MI02V0MvO7AehYXc4BoA3kRzXiTQ+YgQg/dKDH1ddcSMSPUPXUqumowImPU
0pv8amXzhvMLPkcrR8gDQCyn0YemtIBCUfXIA15pPokgP5JRSfkavRo7bm7t+PyIFUnAGrSPZKMD
QjcKpDEDSH3v9jUZgw8kZXv6iz6dbuMcnjGTs3l9PUU+H8U74svRF8byh0fj7VTHB5IuFQVu6Wy1
3ggoJU/cxxGaRc03Vv2XnAHIsenLh0bsJ3JOBPFsLNs4msbetVkCAwEAAaOCAj0wggI5MB8GA1Ud
IwQYMBaAFIT3+nJeiGRmHSiMsHe9DGqfTE1iMBIGA1UdEwEB/wQIMAYBAf8CAQAwggEhBgNVHSAE
ggEYMIIBFDCCARAGCisGAQQBgZNoAQMwggEAMCUGCCsGAQUFBwIBFhlodHRwOi8xd3d3LmFuY2Vy
dC5jb20vY3BzMIHWBggrBgEFBQcCAjCByTANFgZBTkNFUlQwAwIBARqBt0FnZW5jaWEgTm90YXJp
YWwgZGUgQ2VydGlmaWNhY2lvbi4gTGEgZGVjbGFyYWNpb24gZGUgcHJhY3RpY2FzJGRlIGNlcnRp
ZmlhY2lvbiBxdWUgcmlnZSBlbCBmdW5jaW9uYW1pZW50byBkZSBs YSBwcmVzZW50ZSBhdXRvcmlk
YWQgc2UgZW5jdWVudHJhGRpc3BvbmlibGUgZW4gaHR0cDovL3d3dy5hbmNlcnQuY29tL2NwczCB
jwYDVR0fBIGHMIGEMIGBoH+gfYYnaHR0cDovL3d3dy5hbmNlcnQuY29tL2NybC9BTkNFUlROT1Qu
Y3JshihodHRwOi8vd3d3Mi5hbmNlcnQuY29tL2NybC9BTkNFUlROT1QuY3JshihodHRwOi8vd3d3
My5hbmNlcnQuY29tL2NybC9BTkNFUlROT1QuY3JsMA4GA1UdDwEB/wQEAwIBhjAcBgNVHREEFTAT
gRFhbmNlcnRAYWSzZX0lLmNvbTAdBgNVHQ4EFgQUURorbi/OSjhedA2Ue6MN10TjKOwDQYJKoZI
hvcNAQEFBQADggEBAIVA4M6AVIs5gufxX+k5Fy9onCJjDRk2vLIEoKPwb8EAw97WZBgoJNaS1M
4zJ0bJ0TnnnoU/B+kQrOfC5sZLfqzj8nsC3uzBO5dIu0HokBfVmnjLo0pv63ecQQIeohau/A+Su4e
051uJuSVpVnb95U/+uxrRXTTumMB2Ml2NPQxwLXS9WlRvycsYdZaMW7ulk86xX5sSxdXUmyND3l0
qJgcR4fvHBBzXl4mjQNS+yGnZxFRRpm8H6AImr4F4LYO9Z6m6aY+E6Hxojj12Z0hiqXy7S/XzvT
a8H6g55x+c5KK0dNgmrpxcera6I20lzxu2Glr+pj9XJFs7QPpngsZ0=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *ANCERT Certificados Notariales*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados Notariales Corporativos*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Valid from: *Thu Feb 12 14:00:20 CET 2004*

Valid to: *Wed Feb 12 14:00:12 CET 2014*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:66:5D:46:B2:DA:19:4B:6D:27:C9:E8:51:8A:CB:3C:8C:5B:1A:3D:DC:8A:F5:E7:C9:FA:5C:3A:ED:3C:63:82:E0:
A1:EE:AF:8F:12:55:86:E0:8D:04:60:20:EE:53:D0:E7:03:31:6C:73:31:E8:8E:34:D5:72:E0:C7:F4:D9:5D:0C:BC:EE:C0:7A:16:17:7B:80:68:03:79:11:CD:77:D3:43:E6:20:42:0F:DD:28:31:F5:75:D7:12:31:23:D4:3D:75:2A:BA
:6A:30:22:63:D4:D2:9B:FC:6A:65:F3:86:F3:0B:3F:C7:2B:47:C8:03:40:2C:A7:D1:87:A6:B4:90:42:51:F5:C8:00:9D:E9:3E:89:20:3F:92:51:49:FC:5A:BD:1A:3B:6E:6E:ED:F8:FC:89:15:49:C0:1A:B4:8F:64:A3:03:42:37:8A:A
4:31:03:48:7D:EF:F6:35:19:83:0F:24:65:7B:FA:8B:3E:9D:6E:E3:1C:9E:31:93:B3:79:7D:3D:45:3E:1F:C5:3B:E2:CB:D1:17:C6:F2:87:47:E3:4D:54:C7:07:92:2E:15:05:6E:E9:6C:88:DE:A8:28:25:4F:DC:C7:11:9A:45:ED:37:5
6:FD:97:9C:01:C8:B1:E9:CB:87:46:EC:27:72:4E:04:F1:6C:2C:DB:38:9A:C6:DE:B5:59:02:03:01:00:01

Authority Key Identifier *84:F7:FA:72:5E:88:64:66:1D:28:8C:B0:77:BD:0C:6A:9F:4C:4D:62*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.1.3

CPS pointer: http://www.ancert.com/cps

CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en http://www.ancert.com/cps]

CRL Distribution Points

http://www.ancert.com/crl/ANCERTNOT.crl

http://www2.ancert.com/crl/ANCERTNOT.crl

http://www3.ancert.com/crl/ANCERTNOT.crl

Subject Alternative Name *ancert@ancert.com*

Subject Key Identifier *51:1A:2B:6E:2F:CE:4A:38:5E:74:08:B6:51:EE:8C:37:5D:13:8C:AD*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *13:77:15:68:2F:A1:69:5F:25:EA:BC:C0:21:60:B7:2E:34:ED:9A:D3:E9:68:9E:17:7E:2A:E4:3F:83:3E:FC:13*

X509SubjectName

Subject CN: *ANCERT Certificados Notariales Corporativos*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-02-15T01:00:00Z*

3.8.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.3.1.1*

3.8.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.1.3.2.1*

3.8.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.8.4 - History instance n.1 - Status: granted

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Notarial Certificates for legal person*
Name	*[es]*	*Certificados Notariales Reconocidos para personas jurídicas*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados Notariales Corporativos*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*URorbi/OSjhedAi2Ue6MN10TjK0=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

3.8.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.1

3.8.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.2.1

3.8.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

3.8.5 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Notarial Certificates for legal person

Name [es] Certificados Notariales Reconocidos para personas jurídicas

Service digital identities

X509SubjectName

Subject CN: ANCERT Certificados Notariales Corporativos

Subject O: Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

Subject L: Paseo del General Martinez Campos 46-6a planta

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *URorbi/OSjhedAi2Ue6MN10TjK0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

3.8.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.3.1.1*

3.8.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description

[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.3.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.1.3.2.1*

3.9 - Service (withdrawn): Qualified Certificates for the Spanish Notarial Council employees

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates for the Spanish Notarial Council employees*

Name *[es]* *Certificados Reconocidos para empleados del Consejo General del Notariado*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *146686478588265742981622774080664409670*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGFzCCBP+gAwIBAgIQblrJxIZwPEjc3ejdzEaWRjANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQG
EwJFUzFLMEkGA1UEChNCQWdlbmNpYSBOb3Rhcmlhbk CBkZSBDZXJ0aWZpY2FjaW9uIFMuTC4gVW5p
cGVyc29uYWwgLSBDSUYgQjgzMzk10Tg4MSAwHgYDVQQDExdBTkNFUlQgQ2VydGlmaWNhZG9zIENH
TjAcFwtxMTAxMDQxMDI/2MzJaFwt0yMTAxMDQxMDI/2MzJaMIHRMQswCQYDVQQGEwJFUzEPMA0GA1UE
CBMGTWFkcmlkMTcwNQYDVQQHEy5QYXNlbyBkZWwgR2VuZXJhbCBNYXJ0aW5leiBDYW1wb3MgNDYt
NmEgcGxhbnRhMU/swSQYDVQQKE0JBZ2VuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmljYWNpb24gUy5M
LiBVbmlwZXJzb25hbCAtIENJRiBCODMzOTU5ODgxKzApBgNVBAMTIkFOQ0VSVCBDZXJ0aWZpY2Fk
b3MgcGFyYSBlbXBsZWFkb3MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXoITM9QMX
tyST a0p9gC1Y4VJL0UI6TU/bxMloQ06vpt3aEAFvw59FTAoq9lLYW4vhbL8yCRu7vV9EnQTwr/4
ulKACdKlpCcjyNCJeHQmOTYjHGyvz4PSlYUGQdNNpeiHXDOIMABBhVWokyoT8nRtryWCxVqO/xyMv
WKYFJFfOzakfWfCMJ1umw4+W1RzMTPUAhKWIYPgAA4YY5LF7R2MPDltnB/BDLRfivOkjdca+Wu47
mekRpEecxSb+W9MK7P2V3jQMmoddW2pyMD0pd5VZfecosMsaonHkrCAxE7QctFyv33C5ozIlbo5bTh
hUwzK25eO2TTHsMeHfjhtuK0O9HZAgMBAAGjggI9MIICOTAfBgNVHSMEGDAWgBTsVS/IdtJvzDqu
W/AtoWJY0Y0CzDASBgNVHRMBAf8ECDAGAQH/AgEAMIIBIQYDVR0gBIIBGDCCARQwggEQBgorBgEE
AYGTaAQCMIIBADAIBggrBgEFBQcCARYZaHR0cDovL3d3dy5hbmNlcnQuY29tL2NwczCB1gYIKwYB
BQUHAgIwgckwDRYGQUSDRVJUMAMCAQEagbdBZ2VuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmljYWNp
b24uIExhIGRlY2xhcmFiaW9uIGRlIHByYWNQaWNhcyBkZSBhZXI0aWZpYWNpb24gcXVlIHlpZ2Ug
ZWwgZnVuY2lvbmFtaWVudG8gZGUgbGEgcHJlc2VudGUgYXV0b3JpZGFkIHNlIGVuY3VlbnRyYSBk
aXNwb25pYmxlIGVuIGh0dHA6Ly93d3cuYW5jZXJ0LmNvbS9jcHMwgY8GA1UdHwSBhzCBhDCBgaB/
oH2GJ2h0dHA6Ly93d3cuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ0dOLmNybS9oaHR0cDovL3d3dzIu
YW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ0dOLmNybUYoaHR0cDovL3d3dzMuYW5jZXJ0LmNvbS9jcmwv
QU5DRVJUQ0dOLmNybDAOBgNVHQ8BAf8EBAMCAYYwHAYDVR0RBBUwE4ERYW5jZXJ0QGFuY2VydC5j
b20wHQYDVR0OBBYEFFY92w7F8D3TVLADoOH922efiQmvMA0GCSqGSIb3DQEBBQUAA4IBAQB105NO
GeUk1kZVlSOTDC4r9P1haJFLWwwBhNKSACsOPS3/KO5Dt0hyG5xbXXBrGImrbcMvRart5f6K+10u
nIZRFrnpEbcT1EyAK6b4trz2HfGfiYdmZx/LGAYrky7UDFH06GyQeRzL/6Z9WCKzbV0bueocgo8jz
sE4urrlPyqdL17z1op2q6gKwtFe77DdOiELKdkpY8cW1HCCx84pST15U0hKXqPd4VQlKgQInH35q
Yku+AjÜO8Cta0RzciI9M/iQsYS+Z8++xTNSF7SVyb+IW3J+izRHT1TTU+7719ZrvTi353MPYteDv
z6mlLjzLts9siZ9wB8krFtE7bRBKLVbc

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *ANCERT Certificados CGN*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados para empleados*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Valid from: *Tue Jan 04 11:56:32 CET 2011*

Valid to: *Mon Jan 04 11:56:32 CET 2021*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D7:A0:84:CC:F5:03:17:B7:24:93:6B:4A:7D:80:22:18:E1:52:4B:D1:42:04:E9:35:3F:6F:13:25:A1:0D:3A:BE:9B:77:68:40:05:BF:0E:7D:15:30:28:AB:D9:4B:61:6E:2F:85:B2:FC:C8:24:6E:EE:F5:7D:12:74:13:C2:BF:F8:BA:52:80:09:D2:A5:A4:27:23:C8:D0:89:78:74:26:39:36:23:1C:6C:AF:CF:83:D2:95:85:06:41:D3:4D:A5:E8:87:5C:33:88:30:00:41:85:55:A8:93:2A:13:F2:74:6B:C9:60:B1:56:A3:BF:C7:23:2F:58:A6:05:24:57:CE:CD:A9:1F:59:F0:8C:27:5B:A6:C3:8F:96:D5:1C:CC:4C:F5:00:84:A5:A5:60:FA:80:03:86:18:E4:B1:7B:47:63:0F:0E:5B:67:07:F0:43:2D:17:EB:BC:E9:23:75:C6:BE:5A:EE:3B:99:E9:11:A4:47:9B:CE:B8:7E:5B:D3:0A:EC:FD:95:DE:34:0C:9A:87:5D:5B:6A:63:30:3D:29:77:95:59:E9:EC:E8:32:C6:A8:9C:79:2B:08:0C:44:ED:07:2D:17:2B:F7:DC:2E:68:CF:48:68:E5:B4:E1:85:4C:33:2B:6E:5E:3B:64:D3:1E:C3:1E:1D:F8:E1:B6:E2:B4:3B:D1:D9:02:03:01:00:01

Authority Key Identifier

EC:57:9F:C8:76:22:6F:CC:3A:AE:5B:F0:2D:A1:62:58:D1:8D:02:CC

Basic Constraints

IsCA: true - Path length: 0

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.4.2

CPS pointer: http://www.ancert.com/cps

CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en http://www.ancert.com/cps]

CRL Distribution Points

http://www.ancert.com/crl/ANCERTCGN.crl

http://www2.ancert.com/crl/ANCERTCGN.crl

http://www3.ancert.com/crl/ANCERTCGN.crl

Subject Alternative Name

ancert@ancert.com

Subject Key Identifier

56:3D:DB:0E:C5:F0:3D:D3:54:B0:03:A0:E1:FD:DB:67:9F:7D:09:AF

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

78:E1:E1:E0:8C:5D:FC:FA:9A:00:E4:E0:39:CB:D2:0E:D6:D0:63:3D:9C:70:3C:C4:AE:73:4D:C5:73:AF:AA:17

Certificate fields details

Version:

3

Serial Number:

141846559623262997341610771385374835874

X509 Certificate

-----BEGIN CERTIFICATE-----

*MIIGFzCCBP+gAwIBAgIQuranVtSOP6aKQc8J45GEojANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQG
EwJFUzFLMEkGA1UEChNCQWdlbmNpYSBlb3Rhcmlhbi5BLzSBDZXI0aWZpY2FjaW9uIFMuTC4eVW5p
cGVyc29uYWwgLSBDSUYgQjgzMzk10Tg4MSAwHgYDVQQDExdBTkNFUlQgQ2VydGlmaWNhZG9zIENH
TjAeFw0wNDAyMTIxNTAzNDdaFw0xMjAyMTIxNTAzMzlaMIHRMQswCQYDVQQGEwJFUzEPMA0GA1UE
CBMGTWFkcmlkMTcwNQYDVQQHEy5QYXNlbyBkZWwgR2VuZXJhbCBNYXI0aW5leiBDYW1wb3MgNDYt
NmEgcGxhbnRlbMUswSQYDVQQKE0lBZ2VuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlpYWNpb24gIy5M
LiBVbmlwZXJzb25hbCAtIENRiBCODMzOTU5ODgxKzApBgNVBAMTIkFOQ0VSVCBDZXI0aWZpY2Fk
b3MgcGFyYSBlbXBsZWFkb3MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXoITM9QMX
tySTa0p9gCIY4VJL0UIE6TU/bxMloQ06vpt3aEAFvw59FTAoq9lL YW4vhbLSyCRu7vV9EnQTwr/4
ulKACdKlpCcjyNC3eHQmOTYjHGyvz4PSIYUGQdNNpeiHXDOIMAIBBbVWokyoT8nRtyWCxVqOxyMv
WKYTJFOzakfWfCNUIumw4+W1RzMTPUAhKWIYPpA A4YY3L7R2MPDIm8/BDLRfnCQkdca+Wu47
mekRpEeexSh+W9MK7P2V3jQMmoddW2pjMD0pd5VZ6ezoMsaonHkrCAxE7QctFyv33C5oz0lho5bTh
hUwzK25eO2TTHsMeHfjhtuK0O9HZAgMBAAGjggI9MIICOTAIBgNVHSMEGDAWgBTsV5/IdiJvzDqu
W/AtoWIY0Y0CzDASBgNVHRMBAf8ECDAGAQH/AgEAMIIBIQYDVR0gBIIBGDCCARQwggEQBgorBgEE
AYGTaAQCMIIBADAlBggrBgEFBQcCARYZaHR0cDovL3d3dy5ibmNlcnQuY29tL2NwczCB1gYIKwYB
BQUHAgIwgckwDRYGQU5DRVJUMAMCAQEagbdBZ2VuYl2lhIE5vdGFyaWFsIGRlIENlcnRpZmlpYWNp
b24uIExhIGRlY2xhcmFjaW9uIGRlIHByYWN0aWNhcyBkZSBjZXJ0aWZpYWNpb24gcXVlIHJpZ2Ug
ZWwgZnVuY2IvbmFuWVudG8gZGUgbGEgcHJlc2VudGUgYXV0b3JpZGFkIHNlIGVuY3VlbnRyYSBk
aXNvb25pYmxlIGVuIGlhdHlhA6L y93d3cuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ0dOLmNybHYoaHR0cDovL3d3dzMuYW5jZXJ0LmNvbS9jcmwv
oH2GJ2h0dHA6L y93d3cuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ0dOLmNybHYoaHR0cDovL3d3dzIu
YW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ0dOLmNybHAOBgNVHQ8BAf8EBAMCAYYwHAYDVR0RBBUwE4ERYW5jZXJ0QGFuY2VydC5j
b20wHQYDVR0OBBYEFFY92w7F8D3TVLADoOH922ctfQmvMA0GCSqGSIb3DQEBBQUAA4IBAQBKNyN
ucUAtI1/v0WhNrqxz5Ji4pjbbOksVNasAtp6gbrf+YM0obdmVRWai1St1SCdG2Pt4c79oR5Sale
LT7dkuFhMvQcoF2irjhXucvEQfskD+LvYtLemDJnF+DjNAKDtBlnLBCs/+iHZCKdt2Gbzo3Qex/5
LbG4NdN7YXa3oambiVHxpF9Om VYA65O62NlHROiN8ziUnYKY0CJkLpUiADvHdVEDIb9KYBI3fyj
S8h8KWRFd/3ygrFtNWTbbQoJFUWPIFFpEAI8cGnXhOqs55h4wyn7t1ERrhecO4DVess6W2/iji0
N9TU06Q6rdT8sn3DJn3hqARG2GS4NMJt*

-----END CERTIFICATE-----

Signature algorithm:

SHA1withRSA

Issuer CN:

ANCERT Certificados CGN

Issuer O:

Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

Issuer C:

ES

Subject CN:	*ANCERT Certificados para empleados*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*
Valid from:	*Thu Feb 12 16:03:47 CET 2004*
Valid to:	*Sun Feb 12 16:03:39 CET 2012*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D7:A0:84:CC:F5:03:17:B7:24:93:6B:4A:7D:80:22:18:E1:52:4B:D1:42:04:E9:35:3F:6F:13:25:A1:0D:3A:BE:9B:77:68:40:05:BF:0E:7D:15:30:28:AB:D9:4B:61:6E:2F:85:B2:FC:C8:24:6E:EE:F5:7D:12:74:13:C2:BF:F8:BA:52:80:09:D2:A5:A4:27:23:C8:D0:89:78:74:26:39:36:23:1C:6C:AF:CF:83:D2:95:85:06:41:D3:4D:A5:E8:87:5C:33:88:30:00:41:85:55:A8:93:2A:13:F2:74:6B:C9:60:B1:56:A3:BF:C7:23:2F:58:A6:05:24:57:CE:CD:A9:1F:59:F0:8C:27:5B:A6:C3:8F:96:D5:1C:CC:4C:F5:00:84:A5:A5:60:FA:80:03:86:18:E4:B1:7B:47:63:0F:0E:5B:67:07:F0:43:2D:17:EB:BC:E9:23:75:C6:BE:5A:EE:3B:99:E9:11:A4:47:9E:C5:28:7E:5B:D3:0A:EC:FD:95:DE:34:0C:9A:87:5D:5B:6A:63:30:3D:29:77:95:59:E9:EC:E8:32:C6:A8:9C:79:2B:08:0C:44:ED:07:2D:17:2B:F7:DC:2E:68:CF:48:68:E5:B4:E1:85:4C:33:2B:6E:5E:3B:64:D3:1E:C3:1E:1D:F8:E1:B6:E2:B4:3B:D1:D9:02:03:01:00:01*
Authority Key Identifier	*EC:57:9F:C8:76:22:6F:CC:3A:AE:5B:F0:2D:A1:62:58:D1:8D:02:CC*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18920.4.2* *CPS pointer: http://www.ancert.com/cps* *CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en http://www.ancert.com/cps]*
CRL Distribution Points	*http://www.ancert.com/crl/ANCERTCGN.crl* *http://www2.ancert.com/crl/ANCERTCGN.crl* *http://www3.ancert.com/crl/ANCERTCGN.crl*
Subject Alternative Name	*ancert@ancert.com*
Subject Key Identifier	*56:3D:DB:0E:C5:F0:3D:D3:54:B0:03:A0:E1:FD:DB:67:9F:7D:09:AF*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*56:3D:81:58:24:D9:1A:E6:BA:83:AE:08:6A:B5:29:59:80:7D:51:09:8C:25:75:93:38:A3:7D:28:0E:7D:8B:A1*

X509SubjectName

Subject CN:	*ANCERT Certificados para empleados*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-02-15T01:00:00Z*

3.9.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.4.2.1.1*

3.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.9.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates for the Spanish Notarial Council employees*

Name *[es]* *Certificados Reconocidos para empleados del Consejo General del Notariado*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados para empleados*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *Vj3bDsXwPdNUsAOg4f3bZ599Ca8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

3.9.3.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description

[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.4.2.1.1*

3.9.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.9.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates for the Spanish Notarial Council employees*

Name *[es]* *Certificados Reconocidos para empleados del Consejo General del Notariado*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados para empleados*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*Vj3bDsXwPdNUsAOg4f3bZ599Ca8=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2004-11-24T23:00:00Z*

3.9.4.3 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.4.2.1.1*

3.10 - Service (withdrawn): Qualifed Certificates for Public Corporations

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualifed Certificates for Public Corporations*
Name	*[es]*	*Certificados Reconocidos para Corporaciones de Derecho Público*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *285963440239302276055251910074777447 54*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGPzCCBSegAwIBAgIQFYN0nVLbt8xRu8ABCSTEcjANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UE
BhMCRVMxSzBJBgNVBAoTQkFnZW5jaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2lvbiBTLkwuIFVu
aXBlcnNvbmFsIC0gQ0lGIE14MzM5NTk4ODEwMC4GA1UEAxMnQUSDRVUIENvcnBvcmFjaW9uZXMg
ZGUgRGVyZWNobyBQdWJsaWNvMB4XDTA0MDIxMjE0NDQzNFoXDTE0MDIxMjE0NDQyNlowgegxCzAJ
BgNVBAYTAkVTMQ8wDQYDVQQIEwZNYWRyaWQxNzA1BgNVBAcTLlBhc2VvIGRlbCBHZW5lcmFsIE1h
cnRpbmV6IENhbXBvcyA0Ni02YSBwbGFudGExSzBJBgNVBAoTQkFnZW5jaWEgTm90YXJpYWwgZGUg
Q2VydGlmaWNhY2lvbiBTLkwuIFVuaXBlcnNvbmFsIC0gQ0lGIE14MzM5NTk4ODFCMEAGA1UEAxM5
QU5DRVJUIENlcnRpZmlyYWRvcyBwYXJhIENvcnBvcmFjaW9uZXMgZGUgRGVyZWNobyBQdWJsaWNv
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQExtxJMz5oFIQogcnwPtA7jzP1QPMDdlvE
11puAX7lHZbuBSzPDTm9VYoC6QTpn/5IlHmMgkyoAbqZMaf6oXFYEXldzBYU8WrD01kKm2xZW8N/
11Rs1Nc+u7FAxW6QcsMx3jVdlK8JhJx6urFHLHpuOQgs7urVPkbd7qaUcWdatHda/A1EsZubo0YqQ
6abbUhMgSV5MGNdaVm6C+7FovUSd3M7ugZ/JQYIBfiuZbt2TymVIkwHFbPYoq/ph1rvLxWzWQQmms
5lYODAndfz1hwcLeMJ21auKoyUs4f1dTPUcBJQD1obUDI3IWtwSBkwJkUnUq59xgbz158SvU3NLN
tkIBMQIDAQABo4ICPTCCAjkwHwYDVR0jBBgwFoAUjEwcNwyxn9KsRAs6vgLP9l0ZpUwEgYDVR0T
AQH/BAgwBgEB/wIBADCCASEGA1UdIASCARgwggEUMIIBEAYKKwYBBAGBk2gDATCCAQAwJQYIKwYB
BQUHAgEWGWh0dHA6Ly93d5zyYW5jZXI0LmNvb59ycHMwgdYGCCsGAQUFBwICMIHJMA0WBkFOQ0VS
VDADAgEBGoG3QWdlbmNpYSBOb3Rhcmlhbl BkZSBDZXJlaWZpY2FjaW9uLiBMYSBkZWNsYXJhY2lv
biBkZSBwcmFjdGljYXMgZGUgY2VydGlmaWFjaW9uIHF1ZSByaWdlIGVsIGZ1bmNpb25hbWllbnRv
IGRlIGxhIHByZXNlbnRlIGF1dG9yaWRhZCBzZSBlbmN1ZW50cmEgZGlzcG9uaWJsZSBlbiBodHRw
Oi8vd3d3LmFuY2VydC5jb20vY3BzMIGPBgNVHR8EgYcwgYQwgYGgfGB9hudsdHRwOi8vd3d3LmFu
Y2VydC5jb20vY3JsL0FOQ0VSVFBVQi5jcmyGKGh0dHA6Ly93d3czLmFuY2VydC5jb20vY3JsL0FOQ0VSVFBVQi5jcmywwDgYD
VR0PAQH/BAQDAgGGMBwGA1UdEQQVMBOBEWFuY2VydEBhbmNlcnQuY29tMB0GA1UdDgQWBBSQjHVm
N650Izpa2CTBolbL69U/xDANBgkqhkiG9w0BAQUFAAOCAQEARhw1hJ2jwDGAtzgzdPtqob7XFpt0
HwFpHyZ1fXS1feIqRq53iLncgvqkPBxCcX82pDiFjBHV2NrtyOb+bQrvWyEYNsfErG0z2K4enTSi
pWEMSlW+6V+XzkTgi61bNP+NvVGHlNBc5Pycrr35H6KN+ugTeyo8lVTovBZVWRc7xgOqWrTgNkOj
4Y+6B33DYhpA9v+MyqWpJ+ModcUetgo0FnjG6vQTNQSBuTp5Gm8eiF/1kOa61AEJrWdEDsM0z/T
ZLNGp6S08q8SLgXuUrhRAC++WAIO2FN4lhl57n25V8NvCDBqs5b2ygKjLpvwCx2D38ui8lGTKIDq
eXIqawMGDg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ANCERT Corporaciones de Derecho Publico*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados para Corporaciones de Derecho Publico*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Valid from: *Thu Feb 12 15:44:34 CET 2004*

Valid to: *Wed Feb 12 15:44:26 CET 2014*

Public Key:

```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C6:DC:49:33:3E:68:14:84:28:81:C9:F0:3E:D0:3B:8F:33:F5:40:F3:03:76:5B:C4:D7:5A:6E:01:7E:E5:1D:96:EE:05:2C:
CF:0D:39:BD:55:8A:02:E9:04:E9:9F:FE:65:7C:79:8C:82:4C:A8:01:BA:99:31:A7:FA:A1:71:58:11:79:5D:CC:16:14:F1:6A:C3:D3:59:0A:9B:6C:59:5B:C3:7F:97:54:72:D4:D7:3E:BB:B1:40:C5:6E:90:7A:C3:31:DE:35:5D:23:
CF:E1:27:1E:AE:AC:51:CB:1E:9B:8E:42:0B:3B:BA:B5:4F:91:B7:7B:A9:A5:1C:59:D6:AD:D1:D6:BF:03:51:2C:66:E6:E8:D1:8A:90:E9:A6:DB:52:13:20:49:5E:4C:18:D7:5A:56:6E:82:FB:B1:68:BD:44:9D:DC:CE:EE:81:9F
:C9:41:82:01:7E:E6:5B:B7:64:F2:99:52:24:C0:71:5B:3D:8A:2A:FE:98:75:AE:F2:F1:5B:35:90:42:69:AC:E6:56:0E:0C:09:DD:7F:3D:61:C1:C2:DE:30:9D:B5:6A:E2:A8:C9:4B:38:7F:57:53:3D:47:01:25:00:F5:A1:B5:03:23:72
:16:B7:04:81:93:0F:E4:52:75:2A:E7:DC:60:6F:3D:79:F1:2B:D4:DC:D2:CD:B6:47:C1:31:02:03:01:00:01
```

Authority Key Identifier *8C:4C:1E:37:0C:B1:9F:D2:AC:44:0B:3A:BE:02:CF:F4:8D:2D:66:95*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.3.1

CPS pointer: http://www.ancert.com/cps

CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en http://www.ancert.com/cps]

CRL Distribution Points

http://www.ancert.com/crl/ANCERTPUB.crl

http://www2.ancert.com/crl/ANCERTPUB.crl

http://www3.ancert.com/crl/ANCERTPUB.crl

Subject Alternative Name

ancert@ancert.com

Subject Key Identifier

90:8C:75:66:37:AE:74:23:3A:5A:D8:27:C1:A2:56:CB:EB:D5:2B:90

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

60:66:75:6C:46:17:4D:9A:4F:CB:86:86:73:35:86:51:87:F8:A4:96:BD:EF:A4:6A:FB:DA:B2:9A:18:70:B6:B4

X509SubjectName

Subject CN:

ANCERT Certificados para Corporaciones de Derecho Publico

Subject O:

Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

Subject L:

Paseo del General Martinez Campos 46-6a planta

Subject ST:

Madrid

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

3.10.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description

[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.3.1.1.1*

3.10.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.10.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualifed Certificates for Public Corporations*
Name	*[es]*	*Certificados Reconocidos para Corporaciones de Derecho Público*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados para Corporaciones de Derecho Publico*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*kIx1ZjeudCM6WtgnwaJWy+vVK5A=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-03-09T23:00:00Z*

3.10.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18920.3.1.1.1*

3.10.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualifed Certificates for Public Corporations*
Name	*[es]*	*Certificados Reconocidos para Corporaciones de Derecho Público*

Service digital identities

X509SubjectName

Subject CN:	*ANCERT Certificados para Corporaciones de Derecho Publico*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*kIx1ZjeudCM6WtgnwaJWy+vVK5A=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

3.10.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.3.1.1.1*

3.11 - Service (withdrawn): Spanish Notaries Qualified Certificates

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en]	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Spanish Notaries Qualified Certificates*

Name *[es]* *Certificados Reconocidos de Notario*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *419336586795530447104566592872863759 06*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGDTCCBPWgAwIBAgIQH4wg/x92Rc5eUI1u7e5l4jANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQG
EwJFUzFLMEkGA1UECfNCQWdlbmNpYSBOb3Rhcmlhbi0BkZSBDZXJ0aWZpY2FjaW9uIFMuTC4gVW5p
cGVyc29uYWwgLSBDSUYgQjgzMzk10Tg4MSAwHgYDVQQDExdBTkNFUlQgQ2VydGlmaWNhZG9zIENH
TjAeFw0wNDAyMTIxNDUzMTBaFw0xNDAyMTIxNDUzMDJaMIHHMQswCQYDVQQGEwJFUzEPMA0GA1UE
CBMGTWFkcmlkMTcwNQYDVQQHEy5QYXNlbyBkZWwgR2VuZXJhbCBNYXJ0aWSleiBDYW1wb3MgNDYt
NmEgcGxhbnRhMUswSQYDVQQKE0JBZ2VuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlyYWNpb24gUy5M
LiBVbmlwZXJzb25bhCAtIENJRiBCODMzOTU5ODgx1TAfBgNVBAMTGEFOQ0VSVCBDZXJ0aWZpY2Fk
b3MgRkVSTjCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJPgh1jwXsSV6qg5CZZ1kg8
yQsuda3LGI5y+jXD8XReZqaTD0AduoqiPWwzS2LPCn2VuHoXWnGfoF0ZbGYg8kmrhWiI3z6UT7PC
CcbJrKsr6b12fc1bMy50L57D9XnuUIRTyWvu6Jst4/Mt3gcFPEvtOpYp4mxd8wmKiLSlcukOPqF6
x5LFsTFxrE8MQk+0d/sOCYHLh0SwOLy+i4wiNx63t18XJRqTe8SGONK1+fu+szq5lL1K/BdQf7OP
tgYW5TG+UJZa9pzzFux6CkIcGvzGnx/xQD2u+YRIgQHvw48su6UejfBbV/ONSvvGZIe6+CBiPVdh
ZMns872DKKy9EZUCAwEAAaOCAj0wggI5MB8GA1UdIwQYMBaAFOcXn8h2Im/MOq5b8C2hYjRjQLM
MBIGA1UdEwEB/wQIMAYBAf8CAQAwggEhBgNVHSAEggEYMIIBFDCCARAGCisGAQQBgZNoBAEwggEA
MCUGCCsGAQUFBwIBFhlodHRwOi8vd3d3LmFuY2VydC5jb20vY3BzMIHWBggrBgEFBQcCAjCByTAN
FgZBTkNFUlQwAwIBARqBt0FnZW5jaWEgTm90YXJpYWwgZGUgQ2VydGlmaWNhY2lvbsIgTGEgZGVj
bGFyYWNpb24gZGUgcHlhY3RpY2FzIGRlIGNlcnRpZmlhY2lvbsBzdWUgcmlnZSBlbCBmdWSjaW9u
YW1pZW50byBkZSBsYSBwcmVzZW50ZSBhdXRvcmlkYWQgc2UgZW5jdWVudHlhIGRpc3BvbmlibGUg
ZW4gaHR0cDovL3d3dy5hbmNlcnQuY29tL2NwczCBjwYDVR0fBIGHMIGEMIGBoH+gfYYnaHR0cDov
L3d3dy5hbmNlcnQuY29tL2NybC9BTkNFUlRDR04uY3JshihodHRwOi8vd3d3Mi5hbmNlcnQuY29t
L2NybC9BTkNFUlRDR04uY3JshihodHRwOi8vd3d3My5hbmNlcnQuY29tL2NybC9BTkNFUlRDR04u
Y3JsMA4GA1UdDwEB/wQEAwIBhjAcBgNVHREEFTATgRFhbmNlcnRAYW5jZXJ0LmNvbTAdBgNVHQ4E
FgQUmeVcgroY5Yz3iBve0MKtbUayuKYwDQYJKoZIhvcNAQEFBQADggEBAHdaZkqRAY1zlquIAe8h
SDgV9Zk6ekMUyuP87DF6fxvKgv5j2aLo+vuAdD4TV8Hk6mcfephnYEa/PMrMdFiuAczNUsc/Fdc
T2KN7/Ra1tVW68q3k2QoZ3KDzrfx6IcuDznWxysesuaOoJVYQY1AxT538h7wf6+4Ki6tP/SOJH
5mlyd3OTLPlKtobudgd2zjX1ee5kcW+QcGqmqelndOw6SNh1g3TH8R0XzY0AyH+YPVfBpS3us+L2
a50cs+wH9Mlz85bFbnQFugSSu5S8K846BFD6nLBnSz2jmzGspyd9R87gsevajzBVeTDrqDDJoZBh
TcaLUr3ZilzJGX74QcM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ANCERT Certificados CGN*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN:	*ANCERT Certificados FERN*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*
Subject C:	*ES*
Valid from:	*Thu Feb 12 15:53:10 CET 2004*
Valid to:	*Wed Feb 12 15:53:02 CET 2014*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:92:4F:82:14:E3:C1:78:92:57:AA:A0:E4:28:99:D6:48:3C:C9:0B:2E:75:AD:CB:1A:5D:F2:FA:35:C3:F1:74:5E:66:A6:93:0F:40:1D:BA:8A:A2:3D:6C:33:4B:62:CF:0A:7D:95:B8:7A:17:5A:71:9F:A0:5D:19:6C:66:20:F2:49:AB:85:68:A5:DF:3E:94:23:B3:C2:09:C6:C9:AC:AB:2B:E9:BD:76:7D:CD:5B:33:2E:74:2F:9E:C3:F5:79:EE:50:84:53:C9:6B:EE:E8:9B:2D:E3:F3:2D:DE:07:05:3C:4B:E2:3A:96:29:E2:6C:5D:F3:09:8A:88:B4:A5:72:E9:0E:3E:A1:7A:C7:92:C5:B1:31:71:AC:4F:0C:42:4F:B4:77:FB:0E:09:81:CB:87:44:B0:38:BC:BE:8B:8C:22:37:1E:B7:B7:5F:17:25:1A:93:7B:C4:86:38:D2:B5:F9:FB:BE:B3:3A:B9:94:BD:4A:FC:17:50:7F:B3:8F:B6:06:16:E5:31:BE:50:96:5A:F6:3C:F3:16:EC:7A:0A:42:1C:1A:FC:C6:9F:1F:F1:40:3D:AE:F9:84:48:81:01:EF:C3:8F:2C:BB:A5:1E:25:F0:5B:55:F3:8D:4A:F7:86:64:87:BA:F8:20:62:3D:57:61:64:C9:EC:F3:BD:83:28:AC:BD:11:95:02:03:01:00:01*
Authority Key Identifier	*EC:57:9F:C8:76:22:6F:CC:3A:AE:5B:F0:2D:A1:62:58:D1:8D:02:CC*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18920.4.1* *CPS pointer: http://www.ancert.com/cps* *CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en http://www.ancert.com/cps]*
CRL Distribution Points	*http://www.ancert.com/crl/ANCERTCGN.crl* *http://www2.ancert.com/crl/ANCERTCGN.crl* *http://www3.ancert.com/crl/ANCERTCGN.crl*
Subject Alternative Name	*ancert@ancert.com*
Subject Key Identifier	*99:E5:5C:82:BA:18:E5:8C:F7:88:1B:DE:D0:C2:AD:6D:46:B2:B8:A6*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*76:C5:27:32:7D:E2:A2:E3:CD:8C:1B:A8:58:2E:EB:C7:18:88:E1:13:06:01:9F:D8:7F:18:D7:7E:55:FC:85:4E*

X509SubjectName

Subject CN:	*ANCERT Certificados FERN*
Subject O:	*Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L:	*Paseo del General Martinez Campos 46-6a planta*
Subject ST:	*Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

3.11.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.4.1.1.1*

3.11.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.11.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Spanish Notaries Qualified Certificates*

Name *[es]* *Certificados Reconocidos de Notario*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados FERN*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *meVcgroY5Yz3iBve0MKtbUayuKY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-03-09T23:00:00Z*

3.11.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.4.1.1.1*

3.11.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Spanish Notaries Qualified Certificates*

Name *[es]* *Certificados Reconocidos de Notario*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados FERN*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *meVcgroY5Yz3iBve0MKtbUayuKY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

3.11.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description

[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.4.1.1.1*

3.12 - Service (granted): Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»*

Name *[en]* *Qualified Time Stamp issued by «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *103080351365719847069090818487523361 8*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHeTCCBWGgAwIBAgIQAMaGiXx4xIAXaeYevj3xUjANBgkqhkiG9w0BAQsFADCBzjELMAkGA1UE
BhMCRVMxRDBCBgNVBAcTOTBhc2VvIGRlIGNlbGVlZW5lcmFsIE1hcnRpbmV6IENhbXBvcyAtNiA2YSBw
bGFudGEgMjgwMTAgTWFkcmlkMUEwPwYDVQQKEzhBZVuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlj
YWNpb24gUy5ML1UuIC0gQ0lGIE4MzM5NTk4ODE2MDQGA1UEAxMtQU5DRVJUIENlcnRpZmlj YWRv
cyBOb3Rhcmlhbi VzIGRlIFNpc3RlbWFzIFYyMB4XDTIwMDEwNzE1MDk1N1oXDT12MDEwNzE1MDk1
N1owZgxCzAJBgNVBAYTAkVTMTwwQgYDVQQKDDNlbGVuY2lhIE5vdGFyaWFsIGRlIENlcnRpZmlj
YWNpw7NuIFMuTC4gVWSpcGVyc29uYWwxGDAWBgNVBGETD1ZBVEVTTLU3dMzM5NTk4ODExMC8GA1UE
AxMoQU5DRVJUIFF1YWxpZmllZCBUaW1lLXN0YW1wIEF1dGhvcml0eSBHMjCCAaIwDQYJKoZIhvcN
AQEBBQADggGPADCCAYoCggGBALXM3XK8tSzMTk7mtSoM1gqZhCa0YKyVb1xj4oMtN8ZRObwjs1t
EPsFvw5E1XSNq5dMz+b3ZxKCfgNzu5wSuKDm6z5i74mOpbenVGfNpzva5gIK4DbTZu3OvR0cbltj
QuDNeLmoaag7rnbubKnMCDeSIqGUA7ubVI09Dpod/0dt1NO/+pIVpSHM0WK/L12uFhbIQ7p7ficu/
PHybKw3ydcF0KFBIiANjCHIzpUO8LNyjXUskP9ynhPCzzdANZXYa1cy05jI0x4Ig6b6nNLKL0NZ
pUhK0DtXK+9L+24LvgHccOjuU5Z+1cLeCplOzMDcM0by/angP60BYVOyctHLc8q22Dhbb2ClCqoT
R/cLs7bVysdGYIM05zI653yr0F2zFhXBg0MGtFtd+QEZdiqYf0frGueeq4RcL7yKw1m3dq07X7l
5dE1bDSZuODAPYt3F4KpxBuc4gDWgokOVMYsvI/vuFjrvTj8uFrgzmcyzHpg/GiMGMCPwu4wyjIO
yCqSIwIDAQABo4ICBTCCAgEwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwDgYDVR0PAQH/BAQDAgeA
MCsGA1UdEAQkMCKADzIwMjAwMTA3MTUwOTU3WoEPMjAyNTAxMDUxNTA5NTdaMH8GCCsGAQUFBwEB
BHMwcTAvBggrBgEFBQcwAYYjaHR0cDovL29jc3AuYWMuYW5jZXJ0LmNvbS9vY3NwLnh1ZGEwPgYI
KwYBBQUHMAKGMmhldHA6Ly9zdXc1YW5jZXJ0LmNvbS9na2kvdjfvY2VydHMvQU5DRVJUQ1NfVjIu
Y3J0MB8GA1UdIwQYMBaAFNs1uTEfd8wxcNycvIVOvqFXwKMAwGA1UdEwEB/wQCMAAwGgYDVR0g
BBMwETAPBg0rBgEEAYGTaAECAwMBMIGXBgNVHR8EgY8wgYwwgYmggYaggYOGKWh0dHA6Ly93d3cu
YW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ1NfVjIuY3JlshipodHRwOi8vd3d3Mi5hbmNlcnQuY29tL2Ny
bC9BTkNFUlRDUl19WMi5jcmwGKmhldHA6Ly93d3cuYW5jZXJ0LmNvbS9jcmwvQU5DRVJUQ1NfVjIu
LmNybDAdBgNVHQ4EFgQUWghH0W+G84avzfuxnYdBeBXA4ZUw3QYDVR0RBB4wHIEacGtpLmV4cGxv
dGFjaW9uQGFuY2VydC5jb20wDQYJKoZIhvcNAQELBQADggIBACRU7SmdboWDGwrskVSxoGVEUKGE
fs7cCzGinMcuChcTP4scrWY2UGCzPNjjn8d/ubetSXFUU4rtVWhHOEL2LSDHdVR/EZUux/0+8knqI
XRwYKf6wjB26RmFj81PuSL7O895UPTpMTbxBSCQmNggCsPJnlDuue2UNYmVTct02Knx61TEbxwte2
U3CwGqhZPsDQFvUjcrXvtg7ZGVwQlE5bUlQZIoiHptXzHMBxI+dYze4IMP75xLv6RgBj0XPidtW
T9IFOWaVjkkBhaIuqIEqnHftjy2nsEczjs/wl0peLVVyXwlx/RqJOrL/ZdzOc7DSrmEBxh2Icd+
CGHElSwHg455UNQpRTNQJXVsrLYxVR8EnMJFllcNDDyGvsmixII4uM/1/OOzmBEQET7P1Q6lU3nC
ZIBS8uEJW8lO++iGkMSBsgRvXSHk/XuZ4mBPN4fi/aQFqvNJw6DyboZOThsgZxhoKWGnPhIX4juo
Gv0Kq2aaZRsYoqrGDU47wVkd7XIG16LnqrVanMQ+MtCZkRXGOumO3QyV2yfk8IZbwrzjdsIIzSJf3
2zmwZ1u8XKkLYgEE/dlMggzDPWCg8Im7cIZ4SgXwrtmnepe4a4uhrOJQJB/tH8Qhq/Kvcl3Te40
0cRNOhGb3DJ3XfBAOy/x+m5UirzDFYmmyhUtbl9/FXMV4FeN

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Certificados Notariales de Sistemas V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Issuer C: *ES*

Subject CN: *ANCERT Qualified Time-stamp Authority G2*

Subject 2.5.4.97: *VATES-B83395988*

Subject O: *Agencia Notarial de Certificación S.L. Unipersonal*

Subject C: *ES*

Valid from: *Tue Jan 07 16:09:57 CET 2020*

Valid to: *Wed Jan 07 16:09:57 CET 2026*

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:B5:CC:DD:72:BC:B5:2C:CC:4E:4E:E6:B5:2A:0C:97:58:2A:66:10:9A:D1:82:B2:55:BD:71:8F:8A:0C:B4:DF:19:44:E
6:F0:8E:CD:6D:10:FB:05:BF:0E:44:D5:74:8D:AB:97:4C:CF:E6:F7:67:12:B2:22:03:73:BB:9C:12:B8:A0:E6:EB:3E:62:EF:89:8E:A5:B7:A7:54:67:CD:A7:3B:DA:E6:09:4A:E0:38:53:66:ED:CE:BD:1D:1C:6E:5B:63:42:EF:C3
:49:E2:E6:A1:A6:A0:EE:BC:5B:BA:12:A7:30:20:DE:4A:5A:86:50:0E:EE:6D:52:0E:F4:3A:68:77:F3:9D:B7:53:4E:FF:EA:48:56:94:87:30:E5:8A:FC:B2:36:B8:58:61:43:BA:7B:7E:CB:BF:3C:7C:9B:2B:0D:F2:75:C1:74:28:5
0:65:88:03:63:08:72:33:A5:43:BC:2C:DC:A3:5D:4B:24:3F:DC:A7:84:F0:B3:CD:D0:0D:65:76:1A:D5:CC:B4:E6:32:48:D3:1E:00:96:06:FA:9C:D2:CA:2F:43:59:A5:48:4A:D0:3B:57:2B:EF:4B:FB:6E:0B:BE:01:DC:70:E8:EE
:53:96:7E:D5:C2:DE:0A:99:4E:CC:C0:DC:33:46:F2:FD:A9:E0:3F:AD:01:61:53:B2:72:D1:CB:7B:CA:B6:D8:38:5B:6F:60:A5:0A:AA:13:47:F7:0B:B3:B6:D5:CA:C7:46:60:83:34:E7:32:3A:E7:7C:AB:D0:5D:B3:16:15:C1:83:
43:06:88:51:6D:77:E4:04:65:D8:AA:61:FD:1F:AC:6B:9E:7A:AE:11:70:BE:F2:2B:0D:66:DD:DA:B4:ED:7E:E5:E5:D1:35:6C:34:99:B8:E0:C0:3D:88:B7:17:82:A9:C4:1B:9C:E2:A0:D6:82:89:0E:54:C6:2C:BD:4B:EE:16:38:E
F:4E:3F:2E:16:B8:33:99:E8:EF:80:7A:60:FC:68:8C:18:C0:8F:C2:EE:30:CA:32:0E:C8:2A:92:23:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Authority Info Access

http://ocsp.ac.ancert.com/ocsp.xuda

http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt

Authority Key Identifier *DB:35:B9:31:1F:FD:F7:7C:C3:17:0D:C9:CB:C8:55:0B:EA:15:7C:0A*

Basic Constraints *IsCA: false*

Certificate Policies *Policy OID: 1.3.6.1.4.1.18920.1.2.3.3.1*

CRL Distribution Points	*http://www.ancert.com/crl/ANCERTCS_V2.crl* *http://www2.ancert.com/crl/ANCERTCS_V2.crl* *http://www3.ancert.com/crl/ANCERTCS_V2.crl*
Subject Key Identifier	*5A:A8:47:D1:6F:86:F3:86:AF:CD:FB:B1:9D:87:41:78:15:C0:E1:95*
Subject Alternative Name	*pki.explotacion@ancert.com*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*26:AE:01:6C:AC:51:81:94:43:93:AC:4E:06:0E:44:FD:AE:A1:34:7A:0C:18:D8:CC:B1:65:BF:80:EF:A5:80:AE*

X509SubjectName

Subject CN:	*ANCERT Qualified Time-stamp Authority G2*
Subject 2.5.4.97:	*VATES-B83395988*
Subject O:	*Agencia Notarial de Certificación S.L. Unipersonal*
Subject C:	*ES*

X509SKI

X509 SK I	*WqhH0W+G84avzfuxnYdBeBXA4ZU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-10-23T02:00:00Z

4 - TSP: Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)

.

TSP Name

Name	*[en]*	*Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*
Name	*[es]*	*Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*

TSP Trade Name

Name	*[en]*	*VATES-Q2826004J*
Name	*[en]*	*CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*
Name	*[es]*	*CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*
Name	*[en]*	*FNMT*
Name	*[es]*	*FNMT*
Name	*[en]*	*FNMT-RCM*
Name	*[es]*	*FNMT-RCM*
Name	*[en]*	*FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*
Name	*[es]*	*FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

PostalAddress

Street Address	*[en]*	*C/ Jorge Juan, 106*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28009*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*C/ Jorge Juan, 106*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28009*

Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.cert.fnmt.es*
URI	*[en]*	*mailto:ceres@fnmt.es*

TSP Information URI

URI	*[en]*	*http://www.cert.fnmt.es/en/home*
URI	*[es]*	*http://www.cert.fnmt.es*

4.1 - Service (withdrawn): Qualified certificates for individuals issued by FNMT-RCM

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates for individuals issued by FNMT-RCM*
Name	*[es]*	*Certificados reconocidos para personas físicas emitidos por la FNMT-RCM*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *921770777*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIC+TCCAmKgAwIBAgIENvEbGTANBgkqhkiG9w0BAQUFADA2MQswCQYDVQQGEwJFUzENMAsGA1UE
ChMERk5NVDEYMBYGA1UECxMPRk5NVCBDbGFzZSAyIENBMB4XDTk5MDMxODE0NTYxOVoXDTE5MDMx
ODE1MjYxOVowNjELMAkGA1UEBhMCRVMxDTALBgNVBAoTBEZOTVQxGDAWBgNVBAsTD0ZOTVQgQ2xh
c2UgMiBDQTCBnTANBgkqhkiG9w0BAQEFAAOBiwAwgYcCgYEAmD+tGTa/TPT7+dkIU/TVv8fqInpY
40bQXcZa+WltjzFe/rQw/lB0rNadHeBixkndFBJ9cQusBsE/IwaH4JCJ1uXjA7LyJ7GfM8iqazZK
o8Q/eUGdi/UYvKz5j1DhWkaodsQ1CdU3zh07jD03MtGy/YhOH6tCbjrbi/xn0lAnVlmECAQOjggEU
MIIBEDARBglghkgBhvhCAQEEBAMCAAcwWAYDVR0fBFEwTzBNoEugSaRHMEUxCzAJBgNVBAYTAkVT
MQ0wCwYDVQQKEwRGTk1UMRgwFgYDVQQLEw9GTk1UIENsYXNlIDIgQ0ExDTALBgNVBAMTBENSTDEw
KwYDVR0QBCQwIoAPMTk5OTAzMTgxNDU2MTlagQ8yMDE5MDMxODE0NTYxOVowCwYDVR0PBAQDAgEG
MB8GA1UdIwQYMBaAFECadkSXdAfErBTLHo1POkV8MNdhMB0GA1UdDgQWBBRAmnZEl3QHxKwUyx6N
TzpFfDDXYTAMBgNVHRMEBTADAQH/MBkGCSqGSIb2fQdBAAQMMAobBFY0LjADAgSQMA0GCSqGSIb3
DQEBBQUAA4GBAGFMoHxZY1m+O5lE8S3DgEeSjXJyJTHa3NgRcbdN531jWS+aqqyuPsQSwvoIkF
sUlyICeA41dpt7PV5Xa3yZgX8vflR64zgjY+IrJT6lodZPjLwVMZGACokIeb4ZoZVUO2ENv8pEx
PqNHPCgFr0W2nSJMJntLfVsV+RlG3whd

-----END CERTIFICATE-----

Signature algorithm:	*SHA1withRSA*
Issuer OU:	*FNMT Clase 2 CA*
Issuer O:	*FNMT*
Issuer C:	*ES*

Subject OU:	*FNMT Clase 2 CA*
Subject O:	*FNMT*
Subject C:	*ES*
Valid from:	*Thu Mar 18 15:56:19 CET 1999*
Valid to:	*Mon Mar 18 16:26:19 CET 2019*
Public Key:	*30:81:9D:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8B:00:30:81:87:02:81:81:00:98:3F:AD:19:36:93:3D:3E:FE:76:42:14:FD:35:6F:F1:FA:AD:22:7A:58:E3:46:D0:5D:C6:5A:F9:62:2D:8F:31:5E:FE:B4:30:FE:50:74:AC:D6:9D:1D:E0:62:C6:49:DD:14:12:7D:71:0B:AC:06:C1:3F:D7:06:87:E0:90:89:D6:E5:E3:03:B2:F2:27:B1:9F:33:C8:AA:6B:36:4A:A3:C4:3F:79:41:9D:89:46:2F:2B:3E:63:D4:38:56:91:AA:1D:B1:0D:42:75:4D:F3:87:4E:E3:0F:4D:CC:B4:6C:BF:62:13:87:EA:D0:9B:8E:B6:E2:FF:19:F4:94:09:D5:96:61:02:01:03*
CRL Distribution Points	*C=ES,O=FNMT,OU=FNMT Clase 2 CA,CN=CRL1*
Authority Key Identifier	*40:9A:76:44:97:74:07:C4:AC:14:CB:1E:8D:4F:3A:45:7C:30:D7:61*
Subject Key Identifier	*40:9A:76:44:97:74:07:C4:AC:14:CB:1E:8D:4F:3A:45:7C:30:D7:61*
Basic Constraints	*IsCA: true*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*62:B9:26:72:66:21:28:32:A8:E2:2D:AB:93:3D:91:C7:01:12:74:AC:F7:17:03:F9:CC:97:83:37:51:A6:E9:4F*

X509SubjectName

Subject OU:	*FNMT Clase 2 CA*
Subject O:	*FNMT*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-09-12T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

TSP Service Definition URI

URI	[en]	http://www.ceres.fnmt.es/dpc
URI	[es]	http://www.ceres.fnmt.es/dpc

4.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.1.2 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificates for individuals issued by FNMT-RCM
Name	[es]	Certificados reconocidos para personas fisicas emitidos por la FNMT-RCM

Service digital identities

X509SubjectName

Subject OU:	FNMT Clase 2 CA
Subject O:	FNMT
Subject C:	ES

X509SKI

X509 SK I	QJp2RJd0B8SsFMsejU86RXww12E=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

4.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates for individuals issued by FNMT-RCM*

Name [es] *Certificados reconocidos para personas físicas emitidos por la FNMT-RCM*

Service digital identities

X509SubjectName

Subject OU: *FNMT Clase 2 CA*

Subject O: *FNMT*

Subject C: *ES*

X509SKI

X509 SK I *QJp2RJd0B8SsFMsejU86RXww12E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

4.2 - Service (withdrawn): Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [es] *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes*

Name [en] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *16*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFaDCCA1CgAwIBAgIBEDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJFUzERMA8GA1UECgwI
Rk5NVC1SQ00xGTAXBgNVBAsMEEFDIFJBSVogRk5NVC1SQ00wHhcNMDgxMTAxMTIxODQwWhcNMjMx
MTAzMTUzODMzWjAxMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1SQ00xDzANBgNVBAsMBkFD
IEFQRTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM/Uuxm8YhVFqF59lF5fuQilHGRAD
0QUdvD/vsdl6TmWS4sfy85Dj86ZXkiVdJzQWoelEJ1QpCIAbMBy1L1C2oiN6zJ7ONtkEkLJHFEC
a6LSlmnUttrQqdywbvKjChsCMDRFlCrG8cdKyh9yPY2MTQ/uAajRwCo4x2/SZSn+P+zXl6GgvRv4
2NGLVQt5ZYB0ow2FH3lmHIskqODPNroOWvowPAq12T1oASV9uUc3pvLI3C11kQWOtBkaVfqco
W4T92ZMYzcLPY59j6sLDxFFaV+Df/cK1Hlt/GPo64tw7pmjsdiMgmlz9+8k6XQsdhXvnFKmGIMAp
KGo2B+BJcV8CAwEAAaOCAX8wggF7MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEG
MB0GA1UdDgQWBBRjS3RbB7oZiFaLF/L+XluoIyuIzAfBgNVHSMEGDAWgBT3fcX9xOuG3dkpvUd
oMy/h2CabTA+BgNVHSAENzA1MDMGBFUdIAAwKzApBggrBgEFBQcCARYdaHR0cDovL3d3dy5jZXJ0
LmZubXQuZXMvZHBjcy8wgdQGA1UdHwSBzDCByTCBxqCBw6CBwIaBkGxkYXA6Ly9sZGFwZm5tdC5j
ZXJ0LmZubXQuZXMvQ049Q1JMLE9VPUFDJTIwUkFJWiUyMEZOTVQtUkNNLE89Rk5NVC1SQ00sQz1F
Uz9hdXRob3JpdHlISZXZvY2F0aW9uTGlzdDtaWS5hcnk/YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0
cmlsdXRpb25Qb2ludDYraHR0cDovL3dydy5jZXJ0LmZubXQuZXMvY3lscy9BUlkxGTk1UUkNNL mNy
bDANBgkqhkiG9w0BAQUFAAOCAgEAWQpk5BQ4ESQB41qu5AzFdPBEi5k8o+Rnck2fnjK1.xlxsPkwM
kEvFivT/y4lg1rzn/hp/lagdaxA6gsGZj3OVxwLNmBk305ZtPlK7q+svrXKHWO6x5GWhNredd+5
L421Mx97H9BzBuSQVo9RezFlJC7ULn9vcYa94fLy+HNqg9h06hfYVyIMBMwSzRYm8Avb4gzU/4yya
1CvbAtrc6kyHQAnecOM2PPL4y7z10dmOxSNPCTenE/V4CKscx1vO5ns5WYYjao9OAvrD3XuNAXLd9
+LebxsUxUv3Qk8uMOc55Jn0JgiGNLgEDLjLsc/zC0jSmq6RbW30g1COXcJgiupXmV0Bq/SlzCrUm
rT0btoTTX5s8q+hBiqQStl3DVJz8T12KhmCcGlxOEdpsRT5gkLrG0o6yxiJbEb3RWZNF+m8PoVb
S+4NYJVdj9es+9+4qL9Ft+93XzUWxj69CiEzYImn80N9LLnFGyqkKUnE+vww3AQP2I3vsyqmzie
ib5bADIL7WTbIO0Ya2231BN+/UFiqW7ayenwaGjTYmt+2osHUVELJnUi9Wdg1xboGzggkWxz8V
3tapM4NqNqYvmrLsDoS11zQOAADV7ITfjPZSBS5RfIKqr7tqOy09RUpSVxwIYA9EyMP8NszVkZZqC
71ojW/6AtXDcyV9Uw1p0EzK9p4=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject OU: *AC APE*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Wed Nov 05 13:18:40 CET 2008*

Valid to: *Fri Nov 03 16:38:33 CET 2023*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CF:D4:BB:19:BC:62:15:45:A8:5E:7D:94:5E:5F:B9:09:47:19:10:03:D1:05:1D:BC:3F:EF:B1:D2:3A:4E:65:92:E2:C7:F
2:F3:90:E3:F3:A6:57:92:25:5D:27:34:16:A1:E9:44:27:54:29:0A:50:1B:30:1C:B5:2F:50:B6:A2:23:7A:CC:98:D3:38:DB:64:12:42:E5:1C:51:02:6B:A2:FC:96:69:D4:B6:DA:D0:A9:DC:B0:6E:F2:A3:0A:1B:02:30:34:45:20:2C:
C6:F1:C7:4A:CA:1F:72:3D:8D:8C:4D:0F:EE:01:A8:D1:C0:2A:38:C7:6F:D2:65:29:FE:3F:EC:D7:23:A1:A0:BD:1B:F8:D8:D1:8B:55:08:B9:65:8F:C1:D2:8C:36:14:7D:E5:9E:71:C8:B2:4A:8E:0C:F3:6B:A0:E5:AF:A3:03:FF:
22:AD:76:4F:5A:00:49:5F:6E:51:ED:E9:BC:B2:37:0B:5D:64:41:63:AD:06:46:95:22:A7:28:5B:84:FD:D9:93:18:CD:C2:CF:63:9F:63:EA:C2:C3:C4:51:5A:57:E0:DF:FD:C2:B5:1C:8B:7F:18:FA:3A:E2:DC:3B:A6:68:EC:76:2
3:20:98:8C:FD:FB:C9:3A:5D:0B:1D:85:7B:E7:14:A9:86:20:C0:29:28:6A:36:07:E0:49:79:5F:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *63:4B:74:5B:07:BF:E8:66:D1:5A:2C:5F:CB:F9:79:6E:A0:8C:AE:27*

Authority Key Identifier *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.cert.fnmt.es/dpcs/

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FD:01:90:1F:E7:C4:F5:14:D6:36:DF:64:C0:74:4A:A4:02:9D:B9:16:A3:6F:28:47:4C:84:0E:68:07:93:6A:1E*

X509SubjectName

Subject OU: *AC APE*

Subject O: *FNMT-RCM*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

TSP Service Definition URI

URI *[es]* *http://www.ceres.fnmt.es/dpc*

URI *[en]* *http://www.ceres.fnmt.es/dpc*

4.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.5734.3.13*

4.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.2.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[es]	*Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes*
Name	[en]	*Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities*

Service digital identities

X509SubjectName

Subject OU:	*AC APE*
Subject O:	*FNMT-RCM*
Subject C:	*ES*

X509SKI

X509 SK I	*Y0t0Wwe/6GbRWixfy/l5bqCMric=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*
Status Starting Time	*2016-05-29T22:00:00Z*

4.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDAsURN]	*urn:oid:1.3.6.1.4.1.5734.3.13*

4.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[es]	*Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes*
Name	[en]	*Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities*

Service digital identities

X509SubjectName

Subject OU:	*AC APE*
Subject O:	*FNMT-RCM*
Subject C:	*ES*

X509SKI

X509 SK I	*Y0t0Wwe/6GbRWixfy/l5bqCMric=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2010-06-07T00:00:00Z*

4.2.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.5734.3.13*

4.3 - Service (withdrawn): Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles*
Name	*[en]*	*Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *126110685381859351217978824246317433 9*

X509 Certificate

-----BEGIN CERTIFICATE-----

*MIIDLTCCApagAwIBAgIQAPLhXk78tFd1dbiZqW8uwzANBgkqhkiG9w0BAQUFADA1MQswCQYDVQQG EwJFUzENMAsGA1UECgwERk5NVDEXMBUGA1UECwwOQU/MgRkISTUEgTU9WSUwwHhcNMDcxMDIyMTUy ODM5WhcNMjcxMDIyMTQ0MzI3WjA1MQswCQYDVQQGEwJFUzENMAsGA1UECgwERk5NVDEXMBUGA1UE CwwOQUMgRkISTUEgTU9WSUwwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ92KnVjUjtkaRBl HJDAhXriZfn/LSUuvVvXufIJ/a8KKQeBicEq/0X+EmMAHejz52AMLES3/M5K5JIdTWIZs5qbOAA3 a+KwKFb0U/WmSuW7rvKQ/WcfdyAT3sI+j8afM8fs8z3ma4mLqrVSHcATkjOg8yaM3m1cKbOmQuHkn 9HIOBAgMBAACjggE8MIIBODAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4E FgQU89gczFvt/UcPQuPA3lRz1JlvSO8wgfUGA1UdIASB7TCB6jCB5wYJKwYBBAGsZgMIMIHZMDMG CCsGAQUFBwIBFidodHRwOi8vd3d3LmNlcnQuZm5tdC5lcy9kcGNzL2ZtL2RwYy5wZGYwgaEGCCsG AQUFBwICMIGUGoGRU3VqZXRvIGEgbGFzIGNvbmRpY2lvbmVzIGRlIHVzbyBleHB1ZXN0YXMgZW4g bGEgRGVjbGFyYWNpb24gZGUgUHLbY3RpY2FzGRlIENlcnRpZmlyYWNpb24gZGUgbGEgRk5NVCUS Q0gKCBDL0pvcmdlIEp1YW4gMTA2LSAyODAwOS1NYWRyaWQtRXNwYFhKTANBgkqhkiG9w0BAQUF AAOBgQAcC26V2fthdFhCCuI7AVhJQafunEDJMb+vFxpSqslMBl/6GjqumN21Ilq28FMEyX6U/1bU4 9wLwf33B6ueBsfu37h2uYTBjEstrhqLhdjxz29XMcs/7zxYf1gtBkHbGixST7/jjgjSo65u/MEJlSN iZ5U+VPfiaJqRwd9tI9xh0W0oA==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer OU: *AC FIRMA MOVIL*

Issuer O: *FNMT*

Issuer C: *ES*

Subject OU: *AC FIRMA MOVIL*

Subject O: *FNMT*

Subject C: *ES*

Valid from: *Mon Oct 22 17:28:39 CEST 2007*

Valid to: *Fri Oct 22 16:43:27 CEST 2027*

Public Key:

30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:9F:76:2A:75:63:52:3B:64:69:10:65:1C:90:C0:85:7A:E2:65:F9:FF:2D:25:2E:BD:5B:D7:B9:F9:49:FD:AF:0A:29:07:81:89:C1:2A:F F:45:FE:12:63:00:1D:E8:F3:E7:60:0C:2C:44:B7:FC:CE:4A:E4:92:1D:4D:62:19:B3:9A:9B:38:00:37:6B:E2:B0:28:56:F4:51:69:92:B9:6E:EB:BC:A4:23:59:C7:DD:C8:04:F7:B0:8F:A3:F1:A7:CC:F1:FB:3C:CF:79:9A:E2:62:E A:AD:54:87:70:04:E4:8C:E8:3C:C9:A3:37:9B:57:0A:6C:E9:90:B8:79:27:F4:73:81:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *F3:D8:1C:CC:5B:ED:FD:47:0F:42:E3:C0:DE:54:73:D4:99:6F:48:EF*

Certificate Policies

Policy OID: 1.3.6.1.4.1.5734.3.8

CPS pointer: http://www.cert.fnmt.es/dpcs/fm/dpc.pdf

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/Jorge Juan 106- 28009-Madrid-España)]

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *51:EC:D3:8A:33:C7:B4:93:12:97:95:97:20:AF:B3:E9:E7:CD:41:CD:C1:70:09:52:D1:95:88:BD:EC :79:DF:87*

X509SubjectName

Subject OU: *AC FIRMA MOVIL*

Subject O: *FNMT*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

TSP Service Definition URI

URI *[en]* *http://www.ceres.fnmt.es/dpc*

URI *[es]* *http://www.ceres.fnmt.es/dpc*

4.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.3.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados reconocidos para personas fisicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles*

Name *[en]* *Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones*

Service digital identities

X509SubjectName

Subject OU:	*AC FIRMA MOVIL*
Subject O:	*FNMT*
Subject C:	*ES*

X509SKI

X509 SK I	*89gczFvt/UcPQuPA3lRz1JlvSO8=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*
Status Starting Time	*2015-02-24T23:00:00Z*

4.3.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados reconocidos para personas fisicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles*
Name	*[en]*	*Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones*

Service digital identities

X509SubjectName

Subject OU:	*AC FIRMA MOVIL*
Subject O:	*FNMT*
Subject C:	*ES*

X509SKI

X509 SK I	*89gczFvt/UcPQuPA3lRz1JlvSO8=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2010-06-07T00:00:00Z*

4.4 - Service (granted): Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*
Name	*[en]*	*Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG3DCCBMSgAwIBAgIBATANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJFUzERMA8GA1UECgwI
Rk5NVC1SQ00xGTAXBgNVBAsMEEFDIFJBS1vggRk5NVC1SQ00xHhcNMTAwNTIxMDkyNjI0WhcNMjIw
NTIxMDk1MjI2WjBqMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1SQ00xDjAMBgNVBAsMBUNF
UkVTMRIwEAYDVQQFEwlRMjgyNjAwNEoxJDAiBgNVBAMMG0FDIEFkbWluaXN0cmFjacÓzbiBQw7pi
bGljYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJzKT8N13M6D1WHvypwINvv8gC/
LSRX2ZrXwvgfU/oJSMn0TXAfCAdwIUYN8t0GoIRRVv7o5AD1IVg04sP+eeK6Wpl7870SiCeeIPkG
CMvfLSR5jcnZLYZ3IuI3EMuMXc/IEcRT2L603tP/3keGxosqLZ5Q8gVkIkZwTJdm8hypse+NR7Dse
LcPK4wTdmJcWxwN+xcUWUz1IcHeri6tE+pLDZae6HJZHmKwnbQmOAmrAjg301/BIY5iLSZ9QAAjv
LH7qp4opBUsXvYdXkrw0mGPQH1oxz5KlBlmj9DOLhZYQIXF+RgofChI5fWiTmwL5HeCa4eczkHUb
89mi1pvzusECAwEAAaOCArowggK2MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEG
MB0GA1UdDgQWBBQUEzKTK7mMmK1o0zFUQORYXwMbTAtBgNVHSMEGDAWgBT3cX9xOuaGXdkp/Ud
oMy/h2CabTCB6wYDVR0gBIHjMIHgMIHdBgRVHSAAMIHUMCkGCCsGAQUFBwIBFh1odHRwOi8vd3d3
LmNlcnQuZm5tdC5lcy9kcGNzLzCBpgYIKwYBBQUHAgIwgZkMgZZTdWpldGSgYSBsYXMgY29uZGlj
aW9uZXMgZGUgdXNvIGV4cHVlc3RhcyBlbiBsYSBEZWNsYXJhY2nDs24gZGUgUHLDoWN0aWNhcyBk
ZSBDZXJ0aWZpY2FjaCOzbiBkZSBsYSBGTk1ULVIDTSAoIEMvHJpwcmdlIFp1YW4sIDEwN0yOIDAw
OS1NYWRyaWQtRXNwYcOxYSkwgYoGCCsGAQUFBwEBBH4wfDA9BggrBgEFBQcwAYYxaHR0cDovL29j
c3BhcGUuY2VydC5mbm10LmVzL29jc3BhcGUvT2NzcFJlc3BvbmRlcjA7BggrBgEFBQcwAoYvaHR0
cDovL3d3dy5jZXJ0LmZabXQuZXMvY2VydHMvQUNSQUlaRk5NVFJDTS5jcnQwgdQGA1UdIwSBzDCB
yTCBxqCBwe6CBwIaBkGxkYXA6L y9sZGFwZm5tdC5jZXJ0LmZabXQuZXMvQld9Q1JML E9VPUFIDJTTw
UkFJWlUyMEZOTVQtUkNNLE89Rk5NVC1SQ00sQz1FUz9hdXRob3JpdHlSZXZvY2F0aW9uTGlzdDti
aW5hcnk/YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludFraHR0cDovL3d3dy5j
ZXJ0LmZabXQuZXMvY3Jscy9BUkxGTk1UUkNNLmNybDANBgkqhkiG9w0BAQUFAAOCAgEATJlhQSKe
gkhzdgx6dBtnOS8V+kIpB+S6SSGLr62lC62nQfxp+XozIn7iLZGioAbr5cMcXTa3c+cWHlSc1Z
03nLET5jzIR2wVUELiELKxL6Z04ohomi0TqQwv/+OmlkZjKiCqvhVD8MMFxZd7gMwXEv7+uVhJbD
XoX0drsp00QFXKuP/6ColhQzQNnc+qz0BJp5HGwyF4nuZKCl+cL+vnTb7lNOrQkM9Zn0dC8725H
EAtzaNZ0kOpqtNIvIgMuANGGu9hcHYadhIJmCsJfyFXHGvfId0UaDpBfxLEBdr+bdGuGcYIgK9Ob
m7NhYVdWKwGRbFiXis1MCMDIqc6uvurF3xo0HzEcQTgCSxzrV1aANWtNNMNRQp3Sy+dpEIxSsh1
I/LQpeeLPiSnY/Kn/m8rs2BQVCrGj+XABpzOrEvXD61mzIVuGzmzFoMGLKDb27BcI+DU7CEsJ9T
WsIKfH1p0XSRJRHu9w63wCcu1uAdMNNeQiRfdJEBw3B/PztLUntGFj7RKcRCM6CKhtvS1uP6pHt
NczitwejK0A1ctWggRehpzXPI/441hiTxSeS44XiPi1R+VfEewHE52OqhMkGgOcGtSXhFzVi4lb
ogMABVqdV2DNJaGV6A5LOzxmIpvzgiHm/bL1y90Jg7Fr6en7ds/gxbZjyEmAktYPipA=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AC Administración Pública*

Subject SERIAL NUMBER: *Q2826004J*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Fri May 21 11:26:24 CEST 2010*

Valid to: *Sat May 21 11:52:26 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:CA:4F:C3:75:DC:CE:83:D5:61:EF:BF:2A:70:94:DB:EF:F2:00:BF:2D:24:57:D9:9A:D7:C2:F8:1F:53:FA:09:48:C9:F4:AD:70:1F:08:07:70:21:46:0D:F2:DD:06:A1:F4:51:56:FE:E8:E4:00:F5:95:58:34:E2:C3:FE:79:E2:BA:5A:99:7B:F3:B3:92:88:27:9E:10:F9:06:08:CB:DF:2D:2F:39:8F:3C:59:2D:86:77:D1:A0:C4:32:E3:17:7B:F7:C4:71:14:F6:2F:AD:37:B4:F8:B7:91:E1:B1:A2:CA:8B:67:93:B4:81:59:25:91:9C:1F:4D:D9:BC:87:2A:6C:7B:E3:51:EC:3B:1E:2D:C3:CA:E3:04:DD:98:97:16:C7:03:7E:C5:E5:16:53:3D:48:70:77:AB:8B:AB:44:FA:92:C3:65:A7:BA:1C:96:47:98:AC:27:85:09:8E:02:6A:C9:8E:0D:F4:D7:F0:48:63:98:8B:E5:9F:50:00:08:EF:2C:7E:EA:A7:8A:29:05:4B:17:BD:87:57:92:BC:34:98:63:D0:1F:5A:31:CF:92:88:04:89:A3:F4:33:8B:85:96:10:21:71:7E:46:0A:1F:0A:12:39:7D:67:D3:9B:02:F9:1D:E0:9A:E1:EC:E4:1C:9F:DB:F3:D9:E2:D6:9B:F3:BA:C1:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

14:11:E2:B5:2B:B9:8C:98:AD:68:D3:31:54:40:E4:58:5F:03:1B:7D

Authority Key Identifier

F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.cert.fnmt.es/dpcs/

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]

Authority Info Access

http://ocspape.cert.fnmt.es/ocspape/OcspResponder

http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

18:A4:3C:51:D0:81:74:C3:A6:D8:5F:1C:13:18:BD:29:09:75:3E:75:D9:1C:F6:59:9F:73:34:7B:00:70:28:90

Certificate fields details

Version:

3

Serial Number:

2

X509 Certificate

-----BEGIN CERTIFICATE-----

*MIIG3DCCBMSgAwIBAgIBAjANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJFUzERMA8GA1UECgwI
Rk5NVC1SQ00xGTAXBgNVBAsMEEFDIFJBSVogRk5NVC1SQ00wHhcNMTAwNTIxMDkyNjI0WhcNMjIw
NTIxMDk1NzA4WjBqMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1SQ00xDjAMBgNVBAsMBUNF
UkVTMRIwEAYDVQQFEwlRMjgyNjAwNEoxJDAiBgNVBAMMG0FDIEFkbWluaXN0cmFjacOzbiBQw7pi
bGljYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJzKT8N13Mt6D1WHvvypwlNvv8gC/
LSRX2ZzXwvgfUioJSMm0TXAfCAdwIUYN8fOaoRRVv7o5AJTVgt4kP+eeK6Wpl7870S6CzcEPkG
CMvfLS85jzxZLYZ30aDEMuMXe/EcRT2L603tP3keGxosqLZ5O0gVklkZwTfdm8hypse+NR7Dse
LcPK4wTdmJcWxwN+xcUWUz1IcHeri6tE+pLDZae6HJZHmKwnhQmOAmrAjg301/BIY5iLSZ9QAAjv
LH7qp4opBUsXvYdXkrw0mGPQH1oxz5KIBImj9DOLhZYQIXF+RgofChI5fWfTmwL5HeCa4ezkHUb
89ni1pvzusECAwEAAaOCArowggKZMBIGA1UdEwEBwQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEG
MB0GA1UdDgQWBBQUEzKTKTmMnK1o0zFUQORYXwMbTAfBgNVHSMEGDAWgET3tcX9xOuaGJdkpUd
oMy/h2CabTCB6wYDVR0gBIHjMIHgMIHdBgRVHSAAMIHUMCkGCCsGAQUFBwIBFhxodHRwOi8vd3d3
LmNlcnQuZm5tdC5lcy9kcGNzLzCBpgYIKwYBBQUHAgIwgZkMgZZTdWpldG8gYSBsYXMgY29uZGlj
aW9uZXMgZGUgdXNvIGVkcHVlc3RhcyBlbiBsYSBEZWNsYXJhY2nDs24gZGUgUHLDoWN0aWNhcyBk
ZSBDZXJ0aWZpY2FjaCOzbiBkZSBsYSBGTk1ULVJDTSAoIEMnIFjpvcmdlIFjpYW4sIDEwNi0yOIAw
OS1NYWRyaWQtRXNwYcOxYSkwgYoGCCsGAQUFBwEBBH4wfDA9BggrBgEFBQcwAYYxaHR0cDovL29j
c3BhcGUuY2VydC5mbm10LmVzL29jc3BhcGUvT2NzcFJlc3BvbmRlcjA7BggrBgEFBQcwAoYvaHR0
cDovL3d3dy5jZXJ0LmZubXQuZXMvY2VydHMvQUNSQUlaRk5NVFJDTS5jcnQwgdQGA1UdHwSBzDCB
yTCBxqCBw6ZBwIaBkGxkYXA6Ly9sZGFwZm5tdC5jZXJ0LmZubXQuZXMvQ0g9QUMsRVQ9QUMsUEY9UFJDTIw
UkFJWiUyMEZOTVQtUkNNLE89Rk5NVC1SQ00sQz1FUz9hdXRob3JpdHlsZXZvY2F0aW9uTGlzdDti
aW5hcnk/YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludFYraHR0cDovL3d3dy5j
ZXJ0LmZubXQuZXMvY3Jscy9BUkxGTk1UUkNNLmNybDANBgkqhkiG9w0BAQsFAAOCAgEAhfAL4VAy
3vUus88IYy1eRwB73vlyhdQk1vimskfKoF5Wd8Fq7zSfiikSQYugfiwVhB7OL/k8L V7Majzr9Aes29
yqeHd64bUSti8/GZigzWiZAGj6xSX3Vynx46cizQBAlyO0X+3zJD71un719V5nV+gLJU4bZSCDfr
qs5vyCn5KkwWj+TZgqqZ/7aHcoJO3OWSOpQ4o7yeZtZwx1XAaMWSIE3dvMUT1jVc2GfF2Cpk51BU
oUKjDhn2U3PHHATAPkUHU4SqF9/XgLRoYn77HLjp8/TYDjzX9rs6qnbF8DohT00uB07zwL9bcTa0
scqFbZQVRo4ob/2Sm4tAT9ktf7phzgYMQwJ0Xfr+fsB9x/jaPoGvNDiXwkuqVBP56wqDYRpS01
Z7YdmVvrGJPeGXNrFwQCdp4DQgL7APyz50Dp+LjLKRusV9CDB2mELmCZdRKGHX2EC5AIUGWZNRgk
5cEqaRZz2VpgC8tRfEpCFtlZKEakL1y7vbzxuN+JXCZFYNDOM0X8u4dAv6RfvJGcVtZa/QcJvG4d
B7JMOy+lSvWpUEQagugTFp1TrtjycTUj0OEN89YPeQ4eDJBSmA311AGRazD71XKjB5Q8Nul9oHaQa
6ZA83yj74hqOcQ+9FlSAsyASJtGmBXESag0bnjsDQr+jDgUSDlVnA9YTvmiXYZR5y0Q=

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer OU:

AC RAIZ FNMT-RCM

Issuer O:

FNMT-RCM

Issuer C:	*ES*
Subject CN:	*AC Administración Pública*
Subject SERIAL NUMBER:	*Q2826004J*
Subject OU:	*CERES*
Subject O:	*FNMT-RCM*
Subject C:	*ES*
Valid from:	*Fri May 21 11:26:24 CEST 2010*
Valid to:	*Sat May 21 11:57:08 CEST 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:CA:4F:C3:75:DC:CE:83:D5:61:EF:BF:2A:70:94:DB:EF:F2:00:BF:2D:24:57:D9:9A:D7:C2:F8:1F:53:FA:09:48:C9:F4:4D:70:1F:08:07:70:21:46:0D:F2:DD:06:A1:F4:51:56:FE:E8:E4:00:F5:95:58:34:E2:C3:FE:79:E2:BA:5A:99:7B:F3:B3:92:88:27:9E:10:F9:06:08:CB:DF:2D:2F:39:8F:3C:59:2D:86:77:D1:A0:C4:32:E3:17:7B:F7:C4:71:14:F6:2F:AD:37:B4:F8:B7:91:E1:B1:A2:CA:8B:67:93:B4:81:59:25:91:9C:1F:4D:D9:BC:87:2A:6C:7B:E3:51:EC:3B:1E:2D:C3:CA:E3:04:DD:98:97:16:C7:03:7E:C5:E5:16:53:3D:48:70:77:AB:8B:AB:44:FA:92:C3:65:A7:BA:1C:96:47:98:AC:27:85:09:8E:02:6A:C0:8E:0D:F4:D7:F0:48:63:98:8B:E5:9F:50:00:08:EF:2C:7E:EA:A7:8A:29:05:4B:17:BD:87:57:92:BC:34:98:63:D0:1F:5A:31:CF:92:88:04:89:A3:F4:33:8B:85:96:10:21:71:7E:46:0A:1F:0A:12:39:7D:67:D3:9B:02:F9:1D:E0:9A:E1:EC:E4:1C:9F:DB:F3:D9:E2:D6:9B:F3:BA:C1:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*14:11:E2:B5:2B:B9:8C:98:AD:68:D3:31:54:40:E4:58:5F:03:1B:7D*
Authority Key Identifier	*F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.cert.fnmt.es/dpcs/* *CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]*
Authority Info Access	*http://ocspape.cert.fnmt.es/ocspape/OcspResponder* *http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt*
CRL Distribution Points	*ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint* *http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*83:0F:F2:05:AE:69:48:50:59:C3:FB:23:76:A7:F2:F9:EE:1C:2A:61:DE:25:9D:D0:9D:0B:B6:AD:69:F8:88:32*

X509SubjectName

Subject CN:	*AC Administración Pública*
Subject SERIAL NUMBER:	*Q2826004J*
Subject OU:	*CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2019-07-15T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

TSP Service Definition URI

URI *[en]* *http://www.ceres.fnmt.es/dpc*

URI *[es]* *http://www.ceres.fnmt.es/dpc*

4.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.5734.3.3.3.2*

4.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.4.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.5734.3.3.10.1*
Description		

4.4.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

4.4.6 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*
Name	*[en]*	*Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

Service digital identities

X509SubjectName

Subject CN:	*AC Administración Pública*
Subject SERIAL NUMBER:	*Q2826004J*
Subject OU:	*CERES*
Subject O:	*FNMT-RCM*
Subject C:	*ES*

X509SKI

X509 SK I	*FBHitSu5jJitaNMxVEDkWF8DG30=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-09-27T10:00:00Z*

4.4.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.5734.3.3.3.2*

4.4.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.4.6.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.4.6.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.5734.3.3.10.1*

Description

4.4.7 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*

Name [en] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

Service digital identities

X509SubjectName

Subject CN: *AC Administración Pública*

Subject SERIAL NUMBER: *Q2826004J*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *FBHitSu5jJitaNMxVEDkWF8DG30=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

4.4.7.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.5734.3.3.3.2*

4.4.7.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.4.8 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*
Name	*[en]*	*Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

Service digital identities

X509SubjectName

Subject CN:	*AC Administración Pública*
Subject SERIAL NUMBER:	*Q2826004J*
Subject OU:	*CERES*
Subject O:	*FNMT-RCM*
Subject C:	*ES*

X509SKI

X509 SK I	*FBHitSu5jJitaNMxVEDkWF8DG30=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2011-07-27T00:00:00Z*

4.4.8.7 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.5734.3.3.3.2*

4.5 - Service (withdrawn): Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [es] *Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.*

Name [en] *Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *4*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHcTCCBVmgAwIBAgIBBDANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJFUzERMA8GA1UECgwI
Rk5NVC1SQ00xGTAXBgNVBAsMEEFDIFJBSVogRk5NVC1SQ00wHhcNMTAxMTAyMTI0NDExWhcNMjUx
MTAyMTI0NDExWjAxMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1SQ00xDzANBgNVBAMMBkIT
QSBJOTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANF6AL5oCbIY+pMSjOB2fjZ27Wy
7dErzH1Ucgyb13UhS+DyFsKs7PT0Mxfa+q2WcIUasU9rXGDyOB4HAkb0c21pAGOo5PDokDPRVyQH
zN57FWa5W4M5kO/SY1Kxg9HvumZ9ZOzwBNr2LGVTjztC7p1uzgM/IVSXc72XP431mTWe5CRTwA
RVBIefcGhkmv8vrpBfoFHX4kf9PeK10eoZx27uSzBuZlcVx5AS9kHlRuKWPk4cv4zDo+JRfS3mMH
RDGsgiQ1blkxRMFhLgLwYJyln8Ub3VU2CVY6Y0xXVG4jpiB8uFtjdJjHa9bGLp5F47FVrI4aot
XIfmxKeUdlr4eNyrR2DJX8COezZFDO0EARU4IoW5vpmuzVinuT6g1OUgAkSnNZKTJ89zPPZ6G
rbmvLZ5gu6HN3Yxq78mSXPTDCUQzo8e2LUzkqRdZ8z1IGb1gwFDgGva+294TpKsTbPZOkscong
rW1MumqwxQpR4KHWAB/lkvYccGUDCbRL4p0gxT4ESCIKJHFN3lcCeHYv6cuCUsCtb2YDMbM3sCK
qVx1tgSlb2ofICg9B03XurCMJLuMcvTFRP0u5oCLgdj9ZbYnERIxh790Bek02FE7Hul9W7ymz9p
uViuLakeypFwrLjHJCp8dfnp1feqktRnq9r8syqMbQcd7zIBAgMBAAGjggK1MIICbDASBgNVHRMB
AfBECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUR+34Y/CZrr17+fg5cWMv+4jU3
pr0wHwYDVR0jBBgwFoAU933F/cTomht3ZKf1HaDMv4dgmm0wgYsGCCsGAQUFBwEBBH8wfTBBBggr
BgEFBQcwAYY1aHR0cDovL29jc3BJUi0FjYS5jZXJ0LmZubXQuZXMvb2NzcEITQWNhL09jc3BSZXNw
b25kZXJwOAYIKwYBBQUHMAKGLGhtdHA6Ly93d3cuY2VydC5mbm10LmVzL2NlcnRzL0FDUkFJWkZO
TVQuY3J0MIG4BgNVHSAEgbAwgaOwgaoGBFUdIAAwgaEwkQYIKwYBBQUHAgEWHWhtdHA6Ly93d3cu
Y2VydC5mbm10LmVzL2RwY3MvMHQGCCsGAQUFBwICMGgMZIVuZGVyIHRoZSB1c2FnZSBjb25kaXRp
b25zIGFzc2VydGVkIGluIHRoZSBGTk1ULVJDTSBDUFMgKDEwNiwgSm9yZ2UgSnVhbiBzdHJlZXQs
MjgwMDksIE1hZHJpZCwgU3BhaW4pLjCB1AYDVR0fBIHMMIHJMIHGoIHDoIHAhoGQbGRhcDovL2xk
YXBmbm10LmNlcnQuZmStdC5lcy9DTj1JDLkws T1U9QUMlMjBSQUlaJTIwRk5NVC1SQ00sTz1GTk1U
LVJDTSxDPUVTP2F1dGhvcml0eVJldm9jYXRpb25MaXN0O2JpbmFyeT9iYXNlP29iamVjdGNsYXNz
PWNSTERpc3RyaW11dGlvbIBvaW50hitodHRwOi8vd3d3LmNlcnQuZm5tdC5lcy9jcmxzL0FSTEZO
TVRSQ00uY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQBihdMtZ0e6dgOA2VK+QW1ZJla0Ak6RuuvIRXot
RFwUbvAL9AX8uii6PpTUpuRHWuVu3/nsvwzes398tR+IXjc5sjPcMjp9BHZO90d9ZPcf07C0U+FU
iBFRELwCYxjPCHlhRT0/iD7RC+nhCK8Cu62lbEvIhd+K5Cq4wyfPLRb4/jWetmYT7WZtR3A3WD8
fPqEiUgyeBlS1gyeBlS1gEllottvpTob+Hl6T+OQlbxhfRno3hdkC+mmuzCDpHwAxnECWGrkFK1aYBwWGy
dSrd9d1D3UfPwoobxxnqW8TAUEzAo6j3AMTOYpVYyOgynn2lT5Ugm6qOPw14urta6adyn/sTWyU5
EwQZgxSAruwd9UJ3EkchDzr0tn2r0vsrBTbovjG1cdlqrfivRYl7ueS5gWqdFLD2XXAf0VmaCzVAN
BT4I2mI/amvAwyfmzZW9GvyW93IdZUPARvx3ZVswBueW46/hzd+ELN9JfcDS4kMcFO59Dojnkt1M
uc2Z00S/LpoiETwhyeFC1CkC4uoT3L+sy3NndDJLGwYWmjPD6vRFPDTKPv9wovHruGHk4vAuLhFE
T7BabKo2TvTYxUuC2bPOJWOWkkHz72OrVZgHLkbWWAJ73dQgooTODRcjGLfuM9MzKRKDBMoZ9BAa
mvtLOHnCNUY14p//Fh5gQBZ9ICuHDvwT+1HnQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *ISA CA*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Tue Nov 02 13:44:11 CET 2010*

Valid to: *Sun Nov 02 13:44:11 CET 2025*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:7A:00:BE:68:09:B9:58:7F:EA:4C:4A:33:81:D8:8F:59:DB:B5:B2:ED:D1:2D:BC:7D:54:72:0C:9B:D7:75:21:4B:E0
:F2:16:C2:AC:EC:F4:F4:32:E0:3E:AB:65:9C:95:4B:AC:53:DA:D7:18:3C:8E:6F:81:FF:91:BD:22:FF:6D:69:00:63:A8:E4:F0:E8:90:33:D1:62:F4:07:CC:DE:7B:15:66:B9:5A:DE:0C:E6:43:BF:49:8D:4A:97:18:3D:1E:FB:A6:6
7:D6:50:CF:00:4D:AF:62:C6:55:38:F3:B4:2E:E9:D6:EC:E0:33:F9:55:49:77:3B:D9:73:F8:DF:59:93:59:EE:42:45:3C:00:45:50:5F:79:F7:06:86:49:AF:F2:FA:E9:05:FA:05:1D:7E:24:7F:D3:DE:2B:5D:1E:A1:9C:76:EE:E4:B3:0
6:E6:65:71:5C:79:01:2F:64:1E:54:6E:29:63:E4:E1:CB:F8:CC:3A:3E:25:17:D2:DE:63:07:44:31:AC:82:24:35:6E:59:31:44:C1:61:2E:02:F0:60:9C:A5:9F:C5:21:DD:55:36:09:56:24:F5:8D:31:5D:51:B8:8A:98:81:F2:E1:6D:8A:
37:49:8C:76:BD:6C:62:E9:E4:5E:3B:15:5A:C8:E1:AA:2D:5C:87:E6:C4:A7:94:76:5A:F8:78:DC:AB:47:67:C9:5F:C0:8E:7A:B6:45:0C:ED:04:01:15:38:96:85:B9:BE:99:AE:CD:58:A2:8A:E4:FA:83:53:94:80:09:12:9E:23:59:2
9:32:7C:F6:3C:CF:3D:9E:86:7D:B9:AF:2D:9E:60:BB:A1:CD:DD:5C:6A:EF:C9:92:5C:F4:C3:09:44:33:A3:C7:B6:2D:4C:E4:A9:17:59:F3:32:75:19:BD:60:C0:50:E3:1A:F6:BE:DB:DE:13:A6:22:AC:4E:5C:4F:64:E9:2C:72:8
9:E0:AD:6D:4C:BA:6A:B0:C5:0A:51:E0:A1:D6:00:1F:E5:92:F6:1E:70:65:03:09:B4:4B:E2:9D:20:C5:3E:04:48:22:0A:24:71:4D:DE:57:02:78:76:2F:E9:CB:9C:50:9B:02:B5:BD:98:0C:C6:CC:DE:C0:8A:A9:5C:75:B6:04:A5:
6F:6A:1F:94:28:3D:07:4D:D7:BA:B0:8C:24:BB:8C:72:F4:C5:44:FD:2E:E6:80:8B:81:D8:FD:65:B6:27:11:12:31:87:BF:74:05:E9:34:D8:51:3B:1E:E2:3D:5B:BC:AB:9B:3F:69:B9:58:AE:2D:A9:1E:CA:91:70:B4:B8:F8:24:2A:
7C:75:F9:E9:D5:F7:AA:92:D4:67:AB:DA:FC:B3:2A:8C:6D:07:1D:EF:32:01:02:03:01:00:01
```

Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*47:ED:F8:63:F0:99:AF:5E:FE:7E:0E:5C:58:CB:FE:E2:35:37:A6:BD*
Authority Key Identifier	*F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*
Authority Info Access	*http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder* *http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.cert.fnmt.es/dpcs/* *CPS text: [Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).]*
CRL Distribution Points	*ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint* *http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*05:2B:EB:BD:CD:5C:84:7B:FA:0F:6F:B0:EA:22:46:B5:5B:A9:EE:55:E0:2A:2D:48:0B:87:FC:2F:34:2C:84:43*

X509SubjectName

Subject CN:	*ISA CA*
Subject O:	*FNMT-RCM*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

TSP Service Definition URI

URI	*[en]*	*http://www.ceres.fnmt.es/dpc*

URI [es] *http://www.ceres.fnmt.es/dpc*

4.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.5.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.*

Name [en] *Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.*

Service digital identities

X509SubjectName

Subject CN: *ISA CA*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *R+34Y/CZr17+fg5cWMv+4jU3pr0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2016-05-29T22:00:00Z*

4.5.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.*

Name	[en]	*Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.*

Service digital identities

X509SubjectName

Subject CN:	*ISA CA*
Subject O:	*FNMT-RCM*
Subject C:	*ES*

X509SKI

X509 SK I	*R+34Y/CZr17+fg5cWMv+4jU3pr0=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2011-07-27T00:00:00Z*

4.6 - Service (granted): Qualified certificates for individuals issued by AC FNMT Usuarios

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service type description	[en]	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	[en]	*Qualified certificates for individuals issued by AC FNMT Usuarios*
Name	[es]	*Certificados Reconocidos para personas físicas emitidos por AC FNMT Usuarios*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*92211194145327068339343264961472359387*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG2jCCBMKgAwIBAgIQRV864VwhzbpUT4KqR1Hr2zANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQG
EwJFT1ExERMAsGA1UECgwIRk5NVC1SQ00xGTAXBgNVBAsMEEFDIEJBSVcqRk5NVC1SQ00wHhcNMTQx
MDI4MTE0ODU4WhcNMjkxMDI4MTE0ODU4WjBLMQswCQYDVQQGEwJFTzERMAsGA1UECgwIRk5NVC1S
Q00xDjAMBgNVBAsMBUNlcmVzMRkwFwYDVQQDDBBBQyBGTk1UIFVzdWFyaW9zMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnSAEJj37LWkwy9mTl6XlrtRwcu+UvkVr5Y+yC/m6M4Ylr4bx
wNjbt++8b6JBab9wyHhktVSIBa+diYhfsHsHWVWgktOlSzNfPqTPKOmjYtL3UJuoW3AbpDNZJEVFg
EsAkCg5JwXKMjQ7O5CDwIA3VZtbecR4YAOms/Imqm0LSkrWiwwIYF9VnRaqrceAnT/d8KdYCSZ
/9Mc1azWHWN7zJ6MTduZ9PcVjMm70ivilHaohgEUu979by23acx69q7qLPjHkYoGhf2ft1tQqYmjs
9icgwPhrzLyylzzXYy0HoeFns4bi2N+MBTmpf/8HZOK6By3MS2UlCsjXhHhzamwRwIDAQAJBo4IC
yDCCAsQwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFLHUT8Qj
cfpEBQnG6zmP6DWwuCBkMIGYBggrBgEFBQcBAQSBizCBiDBJBggrBgEFBQcwAYY9aHR0cDovL29j
c3Bmbm10cmNtY2EuY2VydCSmbm10LmVzL29jc3Bmbm10cmNtY2EvY2NzcFJlc3BvbmRlcjA7Bggr
BgEFBQcwAoYvaHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY2VydHMvQUNSQUlaRk5NVFJDTS5jcnQw
HwYDVR0jBBgwFoAU933F/cTomht3ZKf1HaDMv4dgmm0wgesGA1UdIASB4zCB4DCB3QYEVR0gADCB
1DApBggrBgEFBQcCARYdaHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvZHBjcy8wgaYGCCsGAQUFBwIC
MIGZDIGWU3VqZXRvIGEgbGFzIGNvbmRpY2lvbmVzIGRlIHVzbyBleHB1ZXN0YXMgZW4gbGEgRGVj
bGFyYWNpw7NuIGRlIFByw6FjdGljYXMgZGUgQ2VydGlmaWNhY2nDs24gZGUgbGEgRk5NVC1SQ00g
KCBDLyBKb3JnZSBKdWFuLCAxMDYtMjgwMDk1TWFkcmlkLUVzcGHDsWEpMIHUBgNVHR8Egcwwgckw
gcugaOygcCGgZBsZGFwOi8vb2dRbzGZubXQuY2VydCSmbm10LmVzL0NOPUNSTCxPVT1BQyUyMFJB
SVolMjBGTk1ULVJDTSxPPUZOTVQtUkNNLEM9RVM/YXV0aG9yaXR5UmV2b2NhdGlvbkxpc3Q7Ymlu
YXJSP2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGK2h0dHA6Ly93d3cuY2Vy
dCSmbm10LmVzL2NybHMvQVJMRk5NVFJDTS5jcmwwDQYJKoZIhvcNAQELBQADggIBAIw9KLTgfg3z
blzaXHc9gGQeTuKSzMnmsv8tgKB4PYRMLGW1L9zxYyyn3VJBz6/8FwuMmoTyCdRdVqKe+YJmwIVe
nF7qg+d8Ro5+X+Zj7att70ZOZGVgb1NAj2pNA+Z+cZrVpUDm31L+3zrIbLypAtEzTx6ATFbJmEg
kpR1AnbWzvuswwUIMUBspR02niCIzqCJVm2u2Uy9kHw+diBJRuwVYppBZavgn7ECNO+vKeIAKZme
+WMd0ZQThkDRYIxFFwYhWFoc1TE+L10nVbEa5jv6oVcauP+2dyLjH/rTdVhb4LnlDKPGKHduQ8
qXuhbxgbIiu8jBT/0n3dWQPFB3oq9+sHIIT9uSUVGrtK+KygGLH5oe8i4GObH7GJUthkUwEYzGi
jg/WmKvm+jg0gnlWT7HiU0K4EWtIdIBl9nNab12ySPVN63q8kCXS3IR8cMR2ZeszLVmPs64tiV
2WKzkrNA+Ltu4Z/UTY4luH+IRevo9reT6790MQvYrCwjSsuND4IXI86/mGESGvhbwECmphe8L/jV
0uZ01yI5mmghedBr5WqKv64EmIXNFVZ23+mh8RFCgqPZsatVaVoBQq1FevOhPMjEvxiMgzPXve2A
3gSmng/UKDcKGzFbyL+veSZhdP854mPk3IPECYZENqAYWXjBIm8UDRmUBt1wpgR

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AC FNMT Usuarios*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Tue Oct 28 12:48:58 CET 2014*

Valid to: *Sun Oct 28 12:48:58 CET 2029*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9D:20:04:26:2D:FB:2D:69:30:CB:D9:93:7F:A5:E5:AE:D4:70:72:EF:94:BE:45:6B:E5:8F:B2:0B:F9:BA:33:86:25:AF:
86:F1:C0:D8:DB:B6:3F:BE:F1:BE:89:05:A6:FD:C3:21:E1:92:D5:52:20:16:BE:76:26:21:7E:C1:EC:59:55:A0:90:E9:52:CC:D2:0F:A9:33:CA:3A:68:D8:B4:BD:D4:26:EA:16:DC:06:E9:0C:D6:49:11:51:60:12:89:64:0A:0E:75:
C1:72:8C:8C:EE:CE:E4:27:C9:C0:80:37:89:5D:9F:6D:E7:91:E1:80:0E:9A:CF:F5:9A:A9:B4:2D:29:2B:5A:2C:30:95:81:7D:56:7F:1A:AA:BF:DE:02:74:FF:77:C2:9D:60:2E:59:FF:D3:1C:D5:AC:D6:1D:63:7B:CC:9E:8C:4D:
DB:99:F4:F7:15:8C:C9:BB:D2:2B:E2:1D:AA:21:80:45:2E:F7:BF:5B:CB:6D:DA:73:1E:BD:AB:BA:8B:3E:31:E4:62:81:A1:7F:67:ED:D6:D4:2A:62:68:EC:F6:27:20:C0:F8:6B:CC:BC:B2:D7:3C:D7:63:2D:07:A1:E1:67:B3:8
6:E2:D8:DF:8C:05:39:A9:7F:F8:BC:1D:93:8A:E8:1C:B7:31:2D:94:94:2B:23:5E:11:E1:CD:A9:B0:47:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *B1:D4:4F:C4:23:79:FA:44:05:09:C6:EB:39:CF:E8:35:B0:B8:20:64*

Authority Info Access

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt

Authority Key Identifier *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.cert.fnmt.es/dpcs/

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *60:12:93:CA:20:B0:9A:03:29:5D:19:62:56:C6:95:3F:F9:EB:A8:11:DB:8E:3C:E1:40:41:3C:1B:FF:E9:A8:69*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

TSP Service Definition URI

URI *[en]* *https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion*

URI *[es]* *https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion*

4.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.6.2 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates for individuals issued by AC FNMT Usuarios*

Name *[es]* *Certificados Reconocidos para personas físicas emitidos por AC FNMT Usuarios*

Service digital identities

X509SubjectName

Subject CN: *AC FNMT Usuarios*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *sdRPxCN5+kQFCcbrOc/oNbC4IGQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-01-01T23:00:00Z*

4.7 - Service (granted): Qualified certificates issued by AC Representación

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by AC Representación*

Name *[es]* *Certificados Reconocidos emitidos por AC Representación*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *129946737925237468182436074897133262369*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG3DCCBMSgAwIBAgIQYcLU1PapmdVkma5ja/WITANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQG
EwJFUzERMA8GA1UECgwIRk5NVC1SQ00tGTAXBgNVBAsMEEFDIEJBSVoqRk5NVC1SQ00tHhcNMTUw
NjMwMDk1MTUzWhcNMjkxMjMxMTA1MTUzWjBNMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1S
Q00xDjAMBgNVBAsMBUNFUkVTMRswGQYDVQQDDBJBQyBSZXByZXNlbnRhY2nDs24wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDCO7E+oU/Ybu1IaWkEQtIFgcRHD/kHavy+XBFdfC/dUzDh9w
7YqvHkYekBPW/YUJQRa4v35IlhujEMCs4cyLnoJy8WyzqTqrSwmNHhMYDjtGywJXbCoSSZVbIuvagW
ig8Nb/x9Y5WGWIY76E9agPAoEYOxOG8h1J6ipNoBbq0R+4N4ODaq57ABY7mUSXb4WgjoVg4WxxZw
0GGLuc8R1idoX1G/VqxvNymeCZ7o1bEwbs7X3NhRsK21w3ju8pkUNZXN6Pkflh9qIslOLiokKbiD
wwAZE4nvU//B8Q8FLYk1sgTQTLET2EQZ308FIECRp3i6Ay4ezc0Yd3FKIDmOxCdDUcDAgMBAAGj
ggLIMIICxDASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQU3FCW
n9cxzkR5Q+WXZfgIGYIMwgZgGCCsGAQUFBwEBBIGLMIGIMEkGCCsGAQUFBzABhj1odHRwOi8v
b2NzcGZubXRyY2FjYS5jZXJ0LmZubXQuZXMvb2NzcGZubXRyY21jYS9PY3NwUmVzcG9uZGVyMDsG
CCsGAQUFBzAChi9odHRwOi8vd3d3LmNlcnQuZm5tdC5lcy9jZXJ0cy9BQ1JBSVpGTk1UUkNNLmNy
dDAfBgNVHSMEGDAWgBT3fcX9xOuaG3dkp/UdoMy/h2CabTCB6wYDVR0gBIHjMIHgMIHdBgRVHSAA
MIHUMCkGCCsGAQUFBwIBFh1odHRwOi8vd3d3LmNlcnQuZm5tdC5lcy9kcGNzLzCB9gYIKwYBBQUH
AgIwgZkMgZZTdWpldG8gYSBsYXMgY29uZGljaW9uZXMgZGUgdXNvIGV4cHVlc3RhcyBlbiBsYSBE
ZWNsYXJhY2nDs24gZGUgUHLDoWN0aWNhcyBkZSBDZXJ0aWZpY2FjacOzbiBkZSBsYSBGTk1ULVJD
TSAoIEMvIEpvcmdlIEp1YW4sIDEwNi0yODAwOS1NYWRyaWQtRXNwYcOxYSkwgdQGA1UdHwSBzDCB
yTCBxqCBw6CBwIaBkGxkYXA6Ly9sZGFwZm5tdC5jZXJ0LmZubXQuZXMvQ0k9QUMlE9VPUFDJTIw
UkFJWiUyMEZOTVQtUkNNLE89RkI5NVC1SQ00sQz1FUz9hdXRob3JpdHlSZXZvY2F0aW9uTGlzdDti
aW5henk/YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludFYraHR0cDovL3d3dy5j
ZXJ0LmZubXQuZXMvY3Jscy9BUkxGTk1UUkNNLmNybDANBgkqhkiG9w0BAQsFAAOCAgEApS/HpvFq
3S42YmpXsoNVxdb+m1/NdjoWVY6MZo9c+UZotZWbatQ+aNOn6/+QfLZk41jD+nEaO1Gk8yAm
eYjyW6Ae7lIVPlVIWQa3fALcgyN7s/U31qPooU7Zv7a5mghpxapWHvtL9yxpLjrtGsZD32qysJ
2pjDqJa5WcWVKF2RS1zy6Bm/9JzlxzTCH03kivP5ltp+cHik/kzJZ+HgPv6BLwO+OYrJ19vGbPuD
GgOj7uJTG3XQlIZchTIgCmNRPKs/HOGOyDmWxm07FmrADQ1NWag3gjoH8xcfAJp9aBnm/UXFJuA
kEOqRASr+ASdpJeDP/iIKpbDdxJpG5YKRwRSb7PnAccstmGxynL+K/0ofxAhbWqC6z7KeGyZB1eV
I1lPhp+xZeJmvFVBjN6s2j7W3+esQkz1T4SdY9RN+c3tBqWFS4UNc7YVe6KVTjzkpcv9szp6vUNQ=
A45i2KGXRLN6/16nA9fujzITRWmX4tOGABo0aL/wBrt3Po89gvZwZRaVQ9Bw/KfEF8eZDhA1MgQK
SPJLSXSI58elHGFLUR2CQMGl+mgIPB0qZUUkRG/RYpZLocczAz6pIkxA3Mt3DIyVtA/YJ0O4ZYp
dbH9zdIZI1RQEWmFrMOrEAWmGIG0SmNpARqOPJsTQJomUcvd3EvA7so2LzLJ+SjjZSo=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AC Representación*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Tue Jun 30 11:51:53 CEST 2015*

Valid to: *Mon Dec 31 11:51:53 CET 2029*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C2:3B:B1:3E:A1:46:1B:B9:32:5A:5A:41:10:B4:81:60:71:11:C3:FE:41:DA:BF:2F:97:04:57:5F:09:D5:33:0E:1F:70:ED:8A:B8:91:87:24:04:F5:BF:61:4D:50:45:AE:2F:DF:91:DB:6A:31:0C:0A:CE:1C:C8:B9:E8:27:2F:16:CB:3A:BB:AA:B4:B0:98:D1:E1:31:80:E3:B4:6C:B0:25:76:C2:A3:94:99:55:B2:30:C9:A8:16:8A:0F:0D:6F:FC:7D:63:95:86:58:86:3B:E8:4F:5A:80:F0:28:11:83:B1:38:6F:21:D4:9E:A2:A4:DA:01:6E:AD:11:FB:83:78:38:36:AA:E7:B0:01:63:B9:94:49:76:F8:5A:08:E8:56:0E:16:C7:16:70:D0:61:8B:B9:CF:11:D6:27:68:5F:51:BF:56:AC:6F:37:29:9E:09:9E:E8:D5:B1:30:6E:CE:D7:DC:D8:51:B0:AD:B5:C3:78:EE:F2:99:14:35:95:CD:E8:F9:1F:96:1F:6A:22:C9:4E:2E:2A:24:29:B8:83:C3:00:19:13:89:EF:53:FF:C1:F1:0F:05:2D:89:35:B2:04:D0:4C:B1:13:D8:44:19:DF:4F:05:94:40:91:A7:78:BA:03:2E:22:7B:37:34:61:DD:C5:28:80:E6:3B:10:9D:0D:47:03:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *DC:50:96:9F:D7:31:89:C9:11:E4:EF:96:5F:F6:5F:82:52:46:62:53*

Authority Info Access

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt

Authority Key Identifier *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.cert.fnmt.es/dpcs/

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8F:D1:6A:17:99:44:D5:D1:D4:20:AF:09:40:5E:DA:7A:BF:2A:9C:74:28:83:E8:C2:F8:9E:0D:90:AF:AF:75:4B*

X509SubjectName

Subject CN: *AC Representación*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

4.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.7.2 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by AC Representación*

Name *[es]* *Certificados Reconocidos emitidos por AC Representación*

Service digital identities

X509SubjectName

Subject CN: *AC Representación*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *3FCWn9cxickR5O+WX/ZfglJGYlM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-08-30T22:00:00Z*

4.8 - Service (granted): Qualified Certificates issued by AC Componentes Informáticos

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by AC Componentes Informáticos*

Name *[es]* *Certificados cualificados emitidos por AC Componentes informáticos*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *701513991919662313744772293237767431 04*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGIjCCBL6gAwIBAgIQNMarBE42mRJRyCULbJTWwDANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQG
EwJFUzERMA8GA1UECgwIRk5NVC1SQ00xGTAXBgNVBAsMEEFDIFJBSVogRk5NVC1SQ00wHhcNMTMw
Nji0MTA1Mjl5WhcNMjgwNjI0MTA1MjI5WjBHMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1S
Q00xJTAjBgNVBAsMHEFDIENvbXBvbmVudGVzIEluZm9ybcOhdGljb3MwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCXVx8rdbF7/xY44CaSqzzGo5BhvzA8knxC73KJYVz1f+CkOvMxMUDu
b8b0h38MDujm/RKZhBNOWbKhxF3U6JZVbcR9xOCcuS/soT80m3BByxAKcZsNka0jCA4XRkgIDaA
FxCHEZI06M0nvXsSOZDPYahbQ3VFCVvcJuhIHdAwSpmceQucRYkR63YgXw7iycCNGivMkAmRS3dlt
qDOmDW/nxiDFq/Jd8VWY7GFkwbbAeqYId8FjN8zIvafumsB9SLFkUjPPMeqfmC7Bdh7HMxLpaOXR
OwH201cmlebiPkn0xSFxXFqwhhr6yN8UQYZ3O/+xdHLrS6DS9+CJUF6d09jAgMBAAGjggLIMIIC
xDASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUGfhYLxTWpsyb
BJgIDUzXqwCnp2UwgZgGCCsGAQUFBwEBBIGLMIGIMEkGCCsGAQUFBzABhj1odHRwOi8vb2NzcGZu
bXRyY21jYS5jZXJ0LmZubXQuZXMvb2NzcGZubXRyY21jYS9PY3NwUmVzcG9uZGVyMDsGCCsGAQUF
BzAChi9odHRwOi8vd3d3LmNlcnQuZm5tdC5lcy9jZXJ0cy9BQ1JBSVpGTk1UUkNNLmNydDAfBgNV
HSMEGDAWgBT3fcX9xOiaG3dkp/UdoMyh2CabTCB6wYDVR0gBIHjMIHgMIHdBgRVHSAAMIHUMCkG
CCsGAQUFBwIBFh1odHRwOi8vd3d3LmNlcnQuZm5tdC5lcy9kcGNzLzCBpgYIKwYBBQUHAgIwgZkM
gZZTdWpldG8gYSBsYXMgY29uZGlzaW9uZGlzaW9uZXMgZGUgdXNvIGV4cHVlc3RhcyBlbiBsYSBEZWNsYXlh
Y2nDs24gZGUgUHLDoWN0aWNhcyBkZSBDZXJ0aWZpY2FjacOzbiBkZSBsYSBGTk1ULVJDTSAoIEMv
IEpvcmdlIEp1YW4sIDEwNi0yODAwOS1NYWRyaWQtRXNwYcOxYSkwgdQGA1UdHwSBzDCByTCBxqCB
w6CBwIaBkGxkYXA6Ly9sZGFwZm5tdC5jZXJ0LmZubXQuZXMvQ049Q1JMLE9VPUFDIJTwUkFJWiU/
MEZOTVQlUkNNLE89Rk5NVC1SQ00bQz1FUz9hdXRob3JpdHlzZXZcY2F0aW9uYGledDtaW5hcnk/
YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludIYraHR0cDov L3d3dy5jZXJ0LmZu
bXQuZXMvY3Jscy9BU kxGTk1UUkNNLmNybDANBgkqhkiG9w0BAQsFAAOCAgEAo2bsQ2xLDcyodieq
jd+uy/lfxDw/MbrAq/ZaNFkIlcypUYamOM4vrm5rz8oLjPCoLkJ48P+nP08Gkcl5Q6q6VFcZLia+
U3gIfXtkyqToQltrVtGCGEf3xAu56XMHGXSdk9vQ0yDnWS7TbUEkp+uvcKewrOvNcpblAzD4eU7
gdOS0w7BagcFRBgTKBw2s3z73fRZtouJg/atmWYtXbBsfNjph+pCh+h5sbSyZUVzO5AemyjpYYYN
MWDQrTXq+7O8ZlPuPaPaNESjEexuzn+VjHG90RlUK1LygARi+Ir0opD2w6erb/hK8Eea7MFdKQ2ASq
NBGJggNo5vfPVvjHiL+Antmb7mQSKL+4YwFU64d4KK9k0C1mbJethDQFKcjTK1vMvnXFiupsIuyT
qwKauo7u2zMKzY4r3YYOW9TpMvLPFIY8ptI5GyNzXlL0F4nseOvduTEPEYqxeNJfpJDPV/DO8Wfx
gdRTy2W3D/UoAulb+Y+nuzGGCtFQrsSMQX487R+aY0nWotlhajefbBcPuxhDfQrg5IafrISVmcJA
plh3tXhh0sz7RbYz6jf1bke4eU5fnrTMtGlVteUL2vjrfUPHW07kBJuaQ7sxORNV3bpHisOnHj+A
riQzCn5vINpSHW6hTm7IfRkbltu/aQrsMuUhP7HE/v+uXe5CuboV5ubZhHU=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject OU: *AC Componentes Informáticos*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Mon Jun 24 12:52:59 CEST 2013*

Valid to: *Sat Jun 24 12:52:59 CEST 2028*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:97:57:1F:2B:75:B1:7B:FF:16:38:E0:26:92:AB:3C:C6:A3:90:61:BF:30:3C:92:7C:42:FF:72:89:61:5C:D3:7F:E0:A4:3A:F3:31:31:40:EE:6F:C6:F4:87:7F:0C:0E:E8:E6:FD:12:99:84:13:4E:59:B2:A1:C4:5D:D4:EB:56:55:85:C4:7D:C4:E0:9C:8A:E4:BF:B2:84:FC:D2:6D:C1:07:2C:40:29:C6:6C:36:46:B4:8C:20:38:5D:19:20:94:36:80:17:10:87:11:9D:3A:30:E9:EF:5E:C4:8E:64:37:CF:61:A8:5B:43:75:45:09:5C:9C:26:E8:65:1D:D0:30:4A:99:9C:79:0C:1C:45:89:11:E9:88:17:C1:38:B2:CC:23:46:8A:F3:0A:02:64:52:DD:D2:2D:A8:33:A6:0D:6F:E7:C6:20:C5:AB:F2:5D:F1:55:98:EC:61:64:C1:B6:C0:7A:A6:08:77:C1:63:37:CC:DF:BD:A7:EE:9E:C0:7D:48:B1:64:52:33:CF:31:EA:9F:98:2E:C1:76:1E:C7:33:12:E9:68:E5:D1:3B:01:F6:D3:57:26:95:E6:E2:3E:49:F4:C5:21:71:5C:5A:B0:86:1A:FA:C8:DF:14:41:86:77:3B:FF:B1:74:72:EB:4B:A0:D2:F7:E0:89:50:5E:9D:D3:D8:A3:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65

Authority Info Access

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt

Authority Key Identifier

F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.cert.fnmt.es/dpcs/

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

F0:38:42:1F:07:F2:0D:63:A2:0D:36:91:E5:A1:78:AB:84:59:EB:E5:70:C1:64:7B:76:90:55:4E:F2:38:76:AB

X509SubjectName

Subject OU:

AC Componentes Informáticos

Subject O:

FNMT-RCM

Subject C:

ES

X509SKI

X509 SK I

GfhYLxTWpsybBJgIDUzXqwCng2U=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2017-09-12T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

4.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.9 - Service (granted): Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *282959601460018754984656648045477620 24*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH5jCCBs6gAwIBAgIQFUmai8lJ48bYOCjXqeCXaDANBgkqhkiG9w0BAQsFADBHMQswCQYDVQQG
EwJFUzERMA8GA1UECgwIRk5NVC1SQ00xJTAjBgNVBAsMHEFDIENvbXBvbmVudGVzIEluZm9vbcOh
dGljb3MwHhcNMTYxMTI1MTIwNDM5WhcNMjIxMTI1MTIwNDM5WjCBujELMAkGA1UEBhMCRVMxRDBC
BgNVBAoMO0bDgUJSSUNBIE5BQ0lPTkFMIERFIE1PTkVEQSBZIFRJTUJSRS1SRUFMIENBU0EgREUg
TEEgTU9ORURBMQ4wDAYDVQQLDAVDRVJFU2zEYMBYGA1UEYQwPVkFURVMtU1T4MjYwMDRKMTswOQYD
VQQDDJBVVRPUkIEQUQgREUgU0VMTEFETyBERSBUSUNUIEkgRk5NVC1SQ00gLSBU1U1UgMjAxNjCC
AaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAKwGyKnMQzIKalrFVi96RAcI37b5xPSfPxZG
/e4OeS5FnanljmJgMZ+Ofv7oRhssoz9n6Gzksl2sx0jXYdk0GyFg+M8kegRQXfI5nZjplhATyU2Z
5b8b3R3HJYwgqX51tHtEvFqH8w74JeIjSXB+H4jDTstBzR756pDh2B24tKKDwkQnaID95N9g0W
gNuHnpNMd8In8GleXRYcHQgBaYcsWCILRQ1UYQ9DHcIvUaR0mr0SEuNPVq7tCLgsgrLpCYG7lZ
ES7NM/o0K61FtRmksIYVf6eRW7z4lz4ck1DGiZ9QP9OF823SncwsWQmEWbUYqGuhN/2oyUd+yH4m
cX0wH8MCOJIyL1sYBcQzIyZGyfFKcS/+C3T9pql+AaI7zN19u2BlhsOvI4vPgUGY2vV+2+cTWBGM
67loq2mgudqxphybbyvJlvt4qHH9I/7teNNsgWp3AGzcYmc93grYIW3d+B7WIwxe3Tmais/5OpZF
z2K9YRFaszZYD0CPkmQxyQIDAQABo4ID2DCCA9QwCQYDVR0TBAIwADCBgQYJKwYBBQUHAQEEdTBz
MDsGCCsGAQUFBzABhi9odHRwOi8vb2NzcGNvbXAuY2VydC5mbm10LmVzL29jc3AvT2NzcFJlc3Bv
bmRlcjA0BggrBgEFBQcwAoYoaHR0cDovL3d3dy5jZXJ0LmZubXQuZXMvY2VydHMvQUNDT01QLmNy
dDCCARYGA1UdIASCAQ0wggEJMIIBBQYKKwYBBAGsZgMIDCB9jApBggrBgEFBQcCARYdaHR0cDov
L3d5dy5jZXJ0LmZubXQuZXMvZHBjcy8wgcgGCCsGAQUFBwICMIG7DIG4QZVydGlmaWNhZGBgcGFy
YSBlbCBTZXJ2aWNpbyBDdWFsaWZpY2FkbyBkZSBTZWxsYWRvIGRlIFRpZWIwbyBkZSBsYSBGTk1U
LVJDTS4gU3VqZXRvIGEgbGFzIGNvbmRpY2lvbmVzIGRlIHVzbyBleHB1ZXN0YXMgZW4gbGEgRFBD
IGRlIGxhIEZOTVQtUkNNIChDL0pvcmdlIEp1YW4gMTA2L TI4MDA5LU1hZHJpZC1Fc3Bhw7FhKTAO
BgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFKH2cG3Mfi07
zDyT4t6Um7FFnx+tMCSGA1UdEAQkMCKAD2twMTYxMTI1MTIwNDQwWoEPMjAyMTExMjUxMjA0Mzla
MIGwBggrBgEFBQcBAwSBozCBoDAIBgYEAI5GAQEwCwYGBACORgEDAgEPMBMGBgQAjkYBBjAJBgcE
AI5GAQYCMHIGBgQAjkYBBTBoMDIWLGh0dHBzOi8vd3d3LmNlcnQuZmStdC5lcy9wZHMvUERTX0NP
TVBfZXMucGRmEwJlczAyFixodHRwczovL3d3dy5jZXJ0LmZubXQuZXMvcGRzL1BEU19DT01QX2Vu
LnBkZhMCZW4wHwYDVR0jBBgwFoAUGibYLxTWpsybBJgIDL2xqwCng2UwgcAGA1UdIwSBZDCB1TCB
0qCBz6CBzIaBnmxkYXA6Ly9sZGFwY29tcC5jZXJ0LmZubXQuZXMvQ049Q1JMMSxPVT1BQyUyMENv
bXBvbmVudGVzJTIwSW5mb3JtYXRpY29zLE89Rk5NVC1SQ00sQz1EUz9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25MaXN0O2JpbmFycF9iYXNlP29namVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvbIBvaW50hilo
dHRwOi8vd3d3LmNlcnQuZmStdC5lcy9jcmxzY29tcC9DUkwxLmNyb2DANBgkqhkiG9w0BAQsFAAOC
AQEAcJMxLz3yjwysGmc/EOccr/0ujfS1FHJLpyUvb8gBftIlb/U3rxFsQpNKB8IbsXCEVOudJPEn
Clk3XOvFacZaSV4gwo7COpaxcv9qXEslj3P9+JBeTR1E4AJbP/G6KuN9Q5llaHounlCTRXJuYB4i
8zZkF1JSySrypP10oSkNttir8sCpaKmKkmflbnsCC6VNfZTAM0lvSXmIga9YktYBEIh9i5A8eVku
BwqvOZQZVpAnOxMpfGXaRzg08mUZLIMrRAozLgSDgjswwd5BotCAb1X+MjILbkGPmGVVtNC1M+2
DqTdmhk49jVQDytL4HMSAg1KBzZ/0KL7lKEpvl8rIQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *AC Componentes Informáticos*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *CERES*

Subject O: *FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

Subject C: *ES*

Valid from: *Fri Nov 25 13:04:39 CET 2016*

Valid to: *Fri Nov 25 13:04:39 CET 2022*

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:AC:06:C8:A9:CC:43:32:0A:6A:5A:C5:56:2F:7A:44:07:25:DF:B6:F9:C4:F4:9F:3F:16:46:FD:EE:0E:79:2E:45:9D:A9:C8:8E:62:60:31:9F:8E:7E:FE:E8:46:1B:2C:A3:3F:67:E8:6C:E4:B2:5D:AC:C7:48:D7:61:D9:34:1B:21:60:F8:CF:24:7A:04:50:5D:F7:EC:9D:98:E9:96:10:13:C9:4D:99:E5:BF:1B:DD:1D:C7:25:8C:20:A9:7E:75:B4:7B:48:12:F1:6A:1F:CC:3B:E0:97:88:8D:25:C1:F8:7E:23:0D:3B:2D:07:34:7B:E7:AA:43:87:60:76:E2:3B:4A:28:3C:24:42:76:89:0F:DE:4D:F6:0D:16:80:DB:87:9E:93:4C:E3:C9:67:F0:69:5E:5D:15:5C:1D:08:01:69:87:2C:58:29:4B:44:E8:D4:2D:84:3D:0C:77:09:BD:46:91:D2:6A:F4:48:4B:8D:3D:8A:AC:EE:D0:8B:82:CA:AB:2E:90:98:1B:B2:19:11:2E:CD:33:FA:34:2B:AD:45:B5:19:A4:B2:56:15:7F:A7:91:5B:BC:F8:97:3E:1C:93:50:C6:7D:9F:50:3F:D3:85:F3:6D:D2:9D:CC:2C:59:09:84:59:B5:18:A8:6B:A1:37:FD:A8:C9:47:7E:C8:7E:26:71:7D:30:1F:C3:02:38:99:72:2F:5B:18:05:C4:33:23:26:46:C9:F1:4A:71:2F:FE:0B:74:FD:A6:A9:7E:01:A2:3B:CC:DD:7D:BB:60:65:86:C3:AF:23:8B:CF:81:41:98:DA:F5:7E:DB:E7:13:58:11:8C:EB:B9:68:AB:69:A0:B9:DA:B1:A6:1C:9B:6F:2B:C9:96:FB:78:A8:71:FD:97:FE:E2:78:D3:6C:81:6A:77:00:6C:DC:62:67:3D:DE:08:98:21:6D:DD:F8:1E:D6:D7:0C:5E:DD:39:9A:8A:CF:F9:3A:96:45:CF:62:BD:61:11:5A:B2:ED:98:0F:40:8F:92:64:31:C9:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Info Access

http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder

http://www.cert.fnmt.es/certs/ACCOMP.crt

Certificate Policies

Policy OID: 1.3.6.1.4.1.5734.3.9.20

CPS pointer: http://www.cert.fnmt.es/dpcs/

CPS text: [Certificado para el Servicio Cualificado de Sellado de Tiempo de la FNMT-RCM. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)]

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *A1:F6:70:6D:CC:7E:8D:3B:CC:3C:93:E2:DE:94:9B:B1:45:9F:1F:9F*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

Authority Key Identifier *19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65*

CRL Distribution Points

ldap://ldapcomp.cert.fnmt.es/CN=CRL1,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crlscomp/CRL1.crl

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *08:F2:93:4C:39:4D:89:DD:B0:CF:C3:86:AA:F5:C5:2E:4F:17:AF:BB:BE:1C:67:A0:36:11:13:2F:80:BE:B7:A9*

X509SubjectName

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *CERES*

Subject O: *FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

Subject C: *ES*

X509SKI

X509 SK I *ofZwbcx+jTvMPJPi3pSbsUWfH58=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2017-09-12T00:00:00Z

4.10 - Service (granted): Qualified Certificates issued by AC SERVIDORES SEGUROS TIPO1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by AC SERVIDORES SEGUROS TIPO1*

Name *[es]* *Certificados cualificados emitidos por AC SERVIDORES SEGUROS TIPO1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *107052318472807923832373279208241425243*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDbTCCAwugAwIBAgIQUImGzbQXDvScG2vVyCTrWzAKBggqhkjOPQQDAzB4MQswCQYDVQQGEwJF
UzERMA8GA1UECgwIRk5NVC1SQ00xDjAMBgNVBAsMBUNlcmVzMRgwFgYDVQRhDA9WQVRFUy1RMjgy
NjAwNEoxLDAqBgNVBAMMI0FDIFJBSVogRk5NVC1SQ00gU0VSVkIET1JFUyBTRUdVUk9TMB4XDTE4
MTIyMDEwMTU0OVoXDTMzMTIyMDEwMTU0OVowcDELMAkGA1UEBhMCRVMxETAPBgNVBAoMCEZOTVQt
UkNNMQ4wDAYDVQQLDAVDZXJlczEYMBYGA1UEYQwPVkFURVMtUTI4MjYwMDRKMSQwIgYDVQQDDBtB
QyBTRVJWSURPUkVTIFNFR1VST1MgVElQTzEwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQ7GlZDbz5O
j5xyUWDC0WHfRa5fJaYDsf3hqmyRoWxsi5iQaG3aaKw/bnYeW1ei6IhC/16LtI8H2Xuta8565GSQ
Af7yOcyoXeRL0qrdqSeTOuu0EcyEmnTWMf+/TQLTvy7OjggFgMIBXDASBgNVHRMBAf8ECDAGAQH/
AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUjEIyQPI5P2sTwXXGXc6GIkQ5b3cwEQYDVR0g
BAowCDAGBgRVHSAAMIGaBggrBgEFBQcBAQSBjTCBjBBBggrBgEFBQcwAYY1aHR0cDovL29jc3Bm
bm10c3NyLmNlcnQuZm5tdC5lcy9vY3Nwc3NyL09jc3BSZXNwb25kZXIwRQYIKwYBBQUHMAKGOWh0
dHA6Ly93d3cuY2VydC5mbm10LmVzL2NlcnRzL0FDUkFJWINFUlZJRE9SRVNTRUdVUk9TLmNydDBG
BgNVHR8EPzA9MDugOaA3hVodHRwOi8vd3d3LmNlcnQuZm5tdC5lcy9jcmxzL0FST1NFUlZJRE9S
RVNTRUdVUk9TLmNybDAfBgNVHSMEGDAWgBQBuS/vvxGGYPJP0EFuq3Mf59JuSTAKBggqhkjOPQQD
AwNoADBlAjB9ZG9la1vG1nY6M7ZutxXbKZVKbCKAwFIDj/+Y/UN4XsyJA+e1tjntR021MciItcC
MQDEcj4K+h5qCFN19m+vVg0O2h1qTS5Cld1ea0JBF5Zee5TZroNF1uWnWKK6FGa0cp4=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *AC RAIZ FNMT-RCM SERVIDORES SEGUROS*

Issuer 2.5.4.97:	*VATES-Q2826004J*
Issuer OU:	*Ceres*
Issuer O:	*FNMT-RCM*
Issuer C:	*ES*
Subject CN:	*AC SERVIDORES SEGUROS TIPO1*
Subject 2.5.4.97:	*VATES-Q2826004J*
Subject OU:	*Ceres*
Subject O:	*FNMT-RCM*
Subject C:	*ES*
Valid from:	*Thu Dec 20 11:15:49 CET 2018*
Valid to:	*Tue Dec 20 11:15:49 CET 2033*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:3B:18:86:43:6F:3E:4E:8F:9C:72:51:60:C2:D1:61:DF:45:AE:5F:8D:A6:03:B1:FD:E1:AA:6C:91:A1:6C:6C:8B:98:90:68:6D:DA:68:AC:3F:6E:76:1E:5B:57:A2:E8:88:42:FC:8E:8B:B4:8F:07:D9:7B:AD:6B:CE:7A:E4:64:90:01:FE:F2:39:CC:A8:5D:E4:4B:D2:AA:DD:A9:27:93:3A:EB:B4:11:CC:84:9E:74:D6:33:EF:D3:40:B4:EF:CB:B3*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*8C:42:32:40:F9:79:3F:6B:13:C1:75:C6:5D:EE:86:22:44:39:6F:77*
Certificate Policies	*Policy OID: 2.5.29.32.0*
Authority Info Access	*http://ocspfnmtssr.cert.fnmt.es/ocspssr/OcspResponder* *http://www.cert.fnmt.es/certs/ACRAIZSERVIDORESSEGUROS.crt*
CRL Distribution Points	*http://www.cert.fnmt.es/crls/ARLSERVIDORESSEGUROS.crl*
Authority Key Identifier	*01:B9:2F:EF:BF:11:86:60:F2:4F:D0:41:6E:AB:73:1F:E7:D2:6E:49*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1E:DB:6B:D9:12:74:88:2D:B7:95:BF:C5:14:F8:AA:BE:10:AD:95:5C:BC:CF:D3:FD:5A:5B:5F:EB:B2:CE:5B:68*

X509SubjectName

Subject CN:	*AC SERVIDORES SEGUROS TIPO1*
Subject 2.5.4.97:	*VATES-Q2826004J*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *jEIyQPl5P2sTwXXGXe6GIkQ5b3c=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2019-07-15T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

4.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

4.11 - Service (granted): Servicio Cualificado de certificados de sello emitidos por “AC Unidades de Sellado de Tiempo”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Servicio Cualificado de certificados de sello emitidos por “AC Unidades de Sellado de Tiempo”*

Name *[en]* *Qualified Certificates eseal issued by “AC Unidades de Sellado de Tiempo”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number:

597171409608801695746634615219643085 70

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJATCCBemgAwIBAgIQLO0aXgKAW7xd34o67KqYWjANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQG
EwJFUzERMA8GA1UECgwIRk5NVC1SQ00xGTAXBgNVBAsMEEFDIFJBSVogRk5NVC1SQ00wHhcNMTkx
MTI4MDg1MDAyWhcNMjkxMTI4MDg1MDAyWjB1MQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1S
Q00xDjAMBgNVBAsMBUNlcmVzMRgwFgYDVQRhDA9WQVRFUy1RMjgyNjAwNEoxKTAnBgNVBAMMIEFD
IFVuaWRhZGVzIGRlIFNlbGxhZG8gZGlsZGlsYCIlbXBvMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEAyEa0GICFLd4/kGN0f8LgxXBGWyCEznOsrmTQbKO9PvNHF6Q1Ig0Hc/zuzQxSC3gf7IIGVb
bgDSojOPcqnKv5JOT4ARax/qUhjSqCgKcTKbCKLW38kQQtPw9N11YGwMNhQYal3ENuj7kGO1edaX
isJATXj+R6al4e2h6zghcMnDnvFCv++9dx//y+0BbY1So/PFcTZCHZ4aWtC428S5b8f3lI7cduVq
O2BHYI+E4ok2y/15YMSoYNmVO9g0eLlma6tm8t2GRAEyHBmthz9jusWN51GbuJXn1iCgd1tYUqEa
u4WQV4t9mucgEjp7MITCM0ffMcAjfqKOJtuSfGZDZPLPxLQMKIv8lS9GOWFpxJZy/Vcfo86PETK77
6zRkVYtkWm4pp41V4oghUOvkHXAyxsKkg9Vdtq8wE+sM0xvS+HdbjGHttpdixu6M4hrAbRgZygF
YVAfLixl3qhJ1W0w1xxy4AOLBAdaAMA/tYh8OO11k8aibjeKB9xcmuEK7yrk57iz+WmwuGIImjg
5EqBz6fwDi5lwx5ZeYkjlg0k1Cni2G0PmUWE+XUyk9tW6YabU8Y0/BDEQbvl6jeVy1jX9AMzAN4m
5Cqdko/iFEuH+StdSkIzpl602UYhj/2KISPFCGJwhNSd2RMQIAxo6CZ/dsUXjXNbRnZmv5UzSA4i
PjsczqMCAwEAAaOCAsUwggLBMA4GA1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMIGV
BggrBgEFBQcBAQSBiDCBhTBJBggrBgEFBQcwAYY9aHR0cDovL29jc3Bmbm10cmNtY2EuY2VydC5m
bm10LmVzL29jc3Bmbm10cmNtY2EvT2NzcFJlc3BvbmRlcjA4BggrBgEFBQcwAoYsaHR0cDovL3d3
dy5jZXJtLmZzZnNQuZXMvY2VydHMvQUNSQUlaRk5NVC5jcnQwIQYDVR0OBBYEFEC5VQSoT39gkO0R
lSXDJfpa9IXVMB8GA1UdIwQYMBaAFPd9xf3E6Jobd2Sn9R2gzL+HYJptMIHrBgNVHSAEgeMwgeAw
gd0GBFUdIAAwgdQwKQYIKwYBBQUHAgEWHWh0dHA6Ly93d3cuY2VydC5mbm10LmVzL2RwY3MvMIGm
BggrBgEFBQcCAjCBmQyBllN1amV0byBhIGxhcyBjb25kaWNpb25lcyBkZSB1c2BgZXhwdWVzdGFz
IGVuIGxhIFRlY2xhcmFjaCOzbiBlZSBjcyBlY3RpY2F2cIGRlIENlcnRpZmlYWNpm7NuIGRlIGxh
IEZOTVQtUkNNICgqQy8gSm9yZ2UgSnVhbiwgMTA2LTI4MDA5LU1hZIUpZC1Fc3Bhw7FhKTCB1AYD
VR0BlHMMIHJMIHJoIHDoIHAhoGQbGRhcDovL2xkYXBmbm10LmNlcnQuZm5tdC5lcy9DTj1DUkws
T1U9QUMlMjBSQUlaJT1wRk5NVC1SQ00sTz1GTk1ULVJDTSxDPUVTP2F1dGhvcmI0eVJldm9jYXRp
b25MaXN0K02JpbmFyeT9iYXNlP29iamVjdGNsYXNzPWNnSTERpc3RyaWJ1dGlhblBvaW50hitodHRw
O8wd3d3LmNlcnQuZm5tdC5lcy9cmxzU0FSTEZOTVRSQ00uY3JsMA0GCSqGSIb3DQEBCwUAA4IC
AQBNFM9IPXNDhmKVlxo4vK6CdL45Gt0+nROnf1KnW83CESo+KiyIEo1quLaG1oe44jWspRJbN1ZE
JQJbNS5ibsuRthF8RN4Bsy1TSNrXETXddKMtqhbihaMrmaW0Ptn1YO+oIAAgfLuHopSiJ2N2rq
q34LerBz/BLB0dhT1y1eK9TRRJlc4vIJsGckaHzC1D90fh7+1amkVmG8GvNLMxvlNKPmlG6dFwXO
9xzeAvzhIDCDjjysdscMOn7m10GPloOwaILFlCqxXVdFIgISv4/o1qp6nFGv4zPuE50ko6dvl
PdoBdRxmGdk5oaBT7ZuFBgUyPMhuWaH5G3M/5wXl6LGVGHNmbxtieBv5HJ8XB0ciIBb+6LSSR/Fr
sQVnqU0QCNIKJYhqW1ghc3wnDazD74KCeqOf&kelNwWZnUocQOpjOAVkPlyOFnvYup9KsNHdK75
O4LGESKqmRfAUQ7Ul0lI5k7A5wJi2z5kvrHQmkSmYtqBIRBu5zX+I5jw3Kgar3r4A8F7ztJ37CEs
xYGo7Kxd2mZcID9cQ1q7WgCb6Aj+1KCbQYL77czTMYRggfUisqSYYaxNYulOF/4Rnb+bch55ulc8
RbAw+Rl0wkeah4BQ+vSBUBmGoJPhC7Z8GRfFCy/2m3ZbozAqHmwkiYktWbmH11TIM+7UEsIfXWCmw
fg==

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer OU:

AC RAIZ FNMT-RCM

Issuer O:

FNMT-RCM

Issuer C:

ES

Subject CN:

AC Unidades de Sellado de Tiempo

Subject 2.5.4.97:

VATES-Q2826004J

Subject OU:

Ceres

Subject O:

FNMT-RCM

Subject C:

ES

Valid from:

Thu Nov 28 09:50:02 CET 2019

Valid to:

Wed Nov 28 09:50:02 CET 2029

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C8:46:B4:18:21:4B:77:8F:E4:18:DD:1F:F0:B8:2C:5C:11:96:C8:21:26:3A:CA:E6:4D:06:CA:3B:D3:EF:34:71:7A:43:5
9:60:D0:77:3F:CE:EC:D0:C5:20:B7:81:FE:C8:20:65:5B:6E:00:D2:A2:33:8F:72:A9:CA:BF:92:4E:4F:80:11:6B:1F:EA:52:18:D2:A8:28:0A:79:32:9B:08:A2:D6:DF:C9:10:42:D3:F0:F4:DD:48:60:6C:0C:36:14:18:6A:5D:C4:36
:E8:FB:90:63:B5:79:D6:97:8A:C2:40:4D:78:FE:47:A6:88:E1:ED:A1:EB:38:21:70:C9:C3:9E:F1:42:BF:EF:BD:77:1F:FF:CB:ED:01:6D:88:B9:A3:F3:C5:79:36:42:1D:9E:1A:5A:D0:B8:DB:CB:39:6F:C7:F7:7C:8E:C2:76:E5:6
A:3B:60:47:60:8F:84:E2:89:36:CB:FD:79:60:CE:68:60:D9:95:43:D8:34:78:B8:67:6B:AD:26:F2:DD:86:44:01:32:1C:19:AD:87:3F:63:BA:F5:8D:E7:51:9B:88:95:E7:4E:20:A0:77:5B:58:52:A1:1A:BB:85:90:57:87:FD:9A:E7:2
0:12:9E:CC:21:30:8C:D1:F7:CC:CC:08:DF:A8:A3:BF:26:E4:9F:19:90:D9:7C:F2:CF:C4:B4:0C:2A:5B:FC:95:2F:46:39:61:69:DD:9C:BF:55:C7:E8:F3:A3:C4:4C:AE:FB:EB:34:64:55:8B:62:91:69:B8:A6:9E:35:57:8A:20:85:4
3:AF:90:75:C0:CB:1B:0A:92:0F:55:76:DA:BC:C0:4F:AC:33:4C:6F:4B:E1:DD:6E:31:87:B6:DA:5D:8B:1B:BA:33:88:6B:01:B4:60:67:28:05:61:50:1F:2E:2C:65:DE:A8:49:D5:6D:30:D7:1C:72:E0:03:8B:04:07:5A:00:C0:3F:7
D:88:7C:38:ED:75:93:C6:A2:6E:37:8A:07:DC:5C:9A:E1:0A:EF:2A:E4:E7:B8:B3:F9:69:B0:BA:21:88:96:68:E0:E4:4A:81:CF:A7:F0:0E:2E:65:C3:1E:59:79:89:23:96:0D:24:D4:29:E2:D8:6D:0F:99:45:84:F9:75:32:93:DB:56:
E9:86:9B:53:C6:34:FC:10:C4:41:BB:E5:EA:37:95:CB:58:D7:F4:03:2B:00:DE:26:E4:2A:9D:92:8F:E2:14:4B:87:F9:2B:78:4A:42:73:A5:FE:B4:D9:46:21:8F:FD:8A:25:23:C5:08:62:70:84:D4:9D:D9:13:10:20:0C:68:E8:26:7F:
E1:B5:17:8D:73:5B:46:76:66:BF:95:33:48:0E:22:3E:3B:1C:CE:A3:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Authority Info Access

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt

Subject Key Identifier

40:B9:55:04:A8:4F:7F:60:90:ED:11:95:25:C3:25:FA:5A:F4:85:D5

Authority Key Identifier

F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.cert.fnmt.es/dpcs/* *CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]*
CRL Distribution Points	*ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint* *http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*9C:E6:30:B3:5F:8A:E2:C6:41:9E:73:4A:D9:D2:FA:30:47:6D:D9:E7:39:4B:1E:93:B2:7F:83:F7:76:A0:24:EA*

X509SubjectName

Subject CN:	*AC Unidades de Sellado de Tiempo*
Subject 2.5.4.97:	*VATES-Q2826004J*
Subject OU:	*Ceres*
Subject O:	*FNMT-RCM*
Subject C:	*ES*

X509SKI

X509 SK I	*QLlVBKhPf2CQ7RGVJcMl+lr0hdU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-06-15T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

4.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.12 - Service (granted): Servicio Cualificado de certificados emitidos por “AC Sector Público”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Servicio Cualificado de certificados emitidos por “AC Sector Público”*

Name *[en]* *Qualified Certificates issued by “AC Sector Público”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *697916248045452963067321503825961419 70*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH8zCCBdugAwIBAgIQNIFgxR9e28td34nKtFczkjANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQG
EwJFUzERMA8GA1UECgwIRk5NVC1SQ00xGTAXBgNVBAsMEEFDIFJBSVogRk5NVC1SQ00wHhcNMTkx
MTI4MDgwODA5WhcNMjkxMTI4MDgwODA5WjBnMQswCQYDVQQGEwJFUzERMA8GA1UECgwIRk5NVC1S
Q00xDjAMBgNVBAsMBUNlcmVzMRgwFgYDVQRhDA9WQVRFUy1RMjgyNjAwNEoxGzAZBgNVBAMMEkFD
IFNlY3RvciBQw7pibGljbzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALiXrTkI+RwQ
tLvjxKUjJI6Gnthgr+3HPWOQjB36laMkldEfQGsVxg6pZdQtW9YQqNEW5OqJ/XxMkExFVt6y9/GJ
OJfT0PFyos7tObuPMw6wk0Yy+1/KZg56dzdsJC1Dybtqpl.k4+tBvyAFMXcwbyWfT0PjZSTnvf5Id
1K2+lEDjQ8LMFOnHQWUBGaOub8lemZnMeGROBYXEWArmjy3wEjVwNxWvaTTYxRw9SbHqfjgOHoLkA
LkMshNM62CGQnHldGBH9w8r4vspF0/XHb3nvq2GWkBhq5fxwu0OzgaBpSiBL4Me6xDJaoeIPxB/m
a3icD+aANiBr92z3zCltTUxe4c33LSqPmnV2GKctADAR3YEcOOPCIXjn5QOdNDQmjPBLCbi8GL5u
5eJ4NZXUiF50LNyoaA9z45BtLSxY2cs+ZCOIsYr8L9X5kITvrAPSIKLlesRYbUnILq1LVkpGaOO
2wzMyoOtp9YEJeaA8punnPI5jSK5n3JIsVesfY0fvq0Dia4V3NLv9jPnOmatbuV1CadT+wuKG0ZV
yoM05zzE5G4B+DH4VWZy0r6WziOc4XfQcTtfMk9hcZEWPJQ5WxIGiUaWEfOvVizrYIzjJd3nXRS
N76+xcHVly6sdy9I17DMODMLLhqn8vR1LJawXM7vNbmNhsSGcex2heeOh6yBpNohAgMBAAGjggLF
MIICwTAOBgNVHQ8BAA8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADCBIQYIKwYBBQUHAQEEgYgw
gYUwSQYIKwYBBQUHMAGGPWhtdHA6Ly9vY3NwZm5tdHJjbWNhLmNlcmQuZm5tdC5lcy9vY3NwZm5t
dHJjbWNhL09jc3BSZXNwb25kZXIwOAYIKwYBBQUHMAKGLGh0dHA6Ly93d3cuY2VydC5mbm10LmVz
L2NlcnRzL0FDUkFJWkZOTVQuY3J0MB0GA1UdDgQWBBTnBO5wkRGSRPkOko9WQx4HHb8EnDAfBgNV
HSMEGDAWgBT3fcX9xOuaG3dkp/UdoMychZabTCB6wYDVR0gBIHfMIHgMIHdBgRVHSAAMIHUMCkG
CCsGAQUFBwIBFh1odHRwOi8vd2d3LmNlcmQuZm5tdC5lcy9kcGNzLzCBhgYIKwYBBQUHAgIwgZkM
gZZTdWpldG8gYSBsYXMgY29uZGljaW9uZXMgZGUgdXNvIGV4cHVlc3RhcyBlbiBsYSBEZWNsYXJh
Y2nDs24gZGUgUHLDoWN0aWNhcyBkZSBDZXJ0aWZpY2FjacOzbiBkZSBsYSBGTk1ULVJDTSAoIEMv
IEpvcmdlIEp1YW4sIDEwNi0yODAwOS1NYWRyaWQtRXNwYcOxYSkwgdQGA1UdHwSBzDCBy TCBxqCB
w6CBwIaBkGxkYXA6Ly9sZGFwZm5tdC5jZXJ0LmZubXQuZXMvQ049Q1JMLE9VPUFDJTIwUkFJWUy
MEZOTVQtUkNNLE89Rk5NVC1SQ00sQz1FUz9hdXRob3JpdHlSZXcY2F0aW9uTGlzdDtiaW5hcnk/
YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludlYraHR0cDovL3d3dy5jZXJ0LmZu
bXQuZXMvY3Jscy9BUkxGTk1UUkNNLmNybDANBgkqhkiG9w0BAQsFAAOCAgEAoiOeh9gNG+m2D5sG
bF42Ykrd3adD2jNwMEzfOy8j3GY9/zIYu749MeNwAg9KVxcNmxNiHHUOqJnzCbPMwMNaS6GcTY
erDsU90C0fsbPmAOIfWQ1RdZWMSDVIOK7lhtRN1pDm0SClCvWt4UtFRnu04VeFlp5Wdi71JisT/
5TwtALk/bsMP56KaZP6NHgvh/CaXu30UxSSaoJ+HPHyDLE2MRpKF8YyiGNEtqslSYZLsicGEdvqc
gDWxnJ8lR0dOMV6T2Aldct0ocAxK+/RUpNx3Dzw9u7zQXwQqR5C7pjpv2Zfz+aSGJWuc/c+XyJRs
ZXBurxMwE4tfKSvAWSBEOM9CaHwMVbhuPyDZqhy2AdLGkpx6TL3QX0eRcsqZrGP79UYNdi3iYo
e8B5btv8qTXnXc4AFYUOgpGFtfOBbX6CwkN7dVng0qy3lfELEB3NYdCJI1omVs1j6UbzW4l7wa0
4JNK3PX3Rm5KgRYy4mxkH3wDAFzMV2021avyPf4SSKwAmQfYpUOQQGcyoSS4Jp2CGTa3+UlgPyO
syPyu98QrAnqt1j11T50xJMgy4lYQDOiL9UmzOYZG/0rawel2iSvCkMHTlknvisXo8cXg7+J1bC0
+hBEoNq+dtWyT+r7PTOGChpQzOHPbye75wBp7lq75dVxe4asXl8YdytrFxI=
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AC Sector Público*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Thu Nov 28 09:48:09 CET 2019*

Valid to: *Wed Nov 28 09:48:09 CET 2029*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:88:97:B5:39:08:F9:1C:10:B4:BB:E3:C4:A5:23:24:8E:86:9D:F8:60:AF:ED:C7:3D:64:10:8C:1D:FA:95:A3:24:95:D1:1F:40:6B:15:C6:0E:A9:65:D4:1F:5B:D6:10:A8:D1:16:E4:EA:89:FD:7C:4C:90:4C:45:56:DE:B2:F7:F1:89:38:97:D3:38:F1:72:CA:CE:ED:39:BB:8F:33:0E:B0:93:46:32:F9:42:99:83:9E:84:6B:F7:71:24:2D:43:C9:BE:A9:23:F9:38:FA:D0:6F:C8:01:4C:5F:3C:1B:BD:67:D3:D0:F8:D9:49:39:EF:7F:9D:5D:D4:AD:BE:20:40:E3:43:C2:CC:14:E9:C7:41:65:01:19:A3:AE:6F:C9:5E:99:99:CC:78:64:4E:05:85:C4:58:0A:E6:8F:2D:F0:12:35:70:37:15:AF:69:37:D8:C5:1C:3D:49:B1:EA:7E:03:87:A0:B9:00:2E:43:2C:84:D3:3A:D8:21:90:9C:79:5D:18:11:FD:C3:CA:F8:BE:CA:45:D3:F5:C7:6F:79:EF:AB:61:96:90:18:6A:E5:FC:70:BB:43:B3:81:A0:69:4A:20:4B:E0:C7:3A:C4:32:5A:A1:E9:4F:C4:1F:E6:6B:78:9C:0F:E6:80:36:20:6B:F7:6C:F7:CC:29:62:4D:4C:5E:E1:CD:F7:2F:CA:8F:9A:75:76:18:A7:2D:00:30:11:DD:81:1C:38:E3:C2:25:78:E7:E5:03:9D:34:34:26:8C:F0:4B:09:B8:BC:18:BE:6E:E5:E2:78:35:95:D4:88:5E:74:2C:DC:A8:A0:0F:73:E3:90:6D:2F:9C:58:D9:EB:3E:64:23:88:B1:8A:FC:2F:D5:F9:92:54:EF:AC:03:F9:94:A2:E5:7A:84:6B:61:B5:27:7C:BA:B5:2D:59:29:19:A3:8E:DB:0C:CC:CA:83:AD:A7:D6:04:25:E6:80:F2:9B:A7:9C:F2:39:8D:22:B9:9F:72:48:B1:57:AC:7D:8D:1F:BE:AD:03:89:AE:15:DC:D2:EF:F6:33:E7:3A:66:AD:6E:E5:75:09:A7:53:FB:0B:8A:1B:46:55:CA:83:34:E7:3C:C4:E4:6E:01:F8:31:F8:55:67:D9:CB:4A:FA:5B:38:8E:73:85:DF:41:C4:E2:7C:C9:3D:85:C6:44:58:F2:50:E5:6C:65:1A:25:2E:58:47:CE:BD:58:B3:AD:82:33:8C:97:77:9D:74:52:37:BE:BE:C5:C1:D5:97:2E:AC:77:2F:48:D7:B0:CC:38:33:0B:2E:1A:A7:F2:F4:75:2C:96:B0:5C:CE:EF:35:B9:8D:86:CE:46:71:EC:76:85:E7:8E:87:AC:81:A4:DA:21:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Info Access

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt

Subject Key Identifier *E7:04:EE:70:91:11:92:44:F9:0E:92:8F:56:43:1E:07:1D:BF:04:9C*

Authority Key Identifier *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.cert.fnmt.es/dpcs/

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *82:65:75:6D:D5:CD:8A:37:EE:61:E4:03:51:28:8E:4B:16:A8:9D:D2:48:C1:EC:4E:BA:25:AA:F1:61:AB:F4:98*

X509SubjectName

Subject CN: *AC Sector Público*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *5wTucJERkkT5DpKPVkMeBx2/BJw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2020-07-28T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

4.12.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.5734.3.17.5*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.5734.3.17.6*

Description

4.12.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.12.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.12.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[es]	Servicio Cualificado de certificados emitidos por “AC Sector Público”
Name	[en]	Qualified Certificates issued by “AC Sector Público”

Service digital identities

X509SubjectName

Subject CN:	AC Sector Público
Subject 2.5.4.97:	VATES-Q2826004J
Subject OU:	Ceres
Subject O:	FNMT-RCM
Subject C:	ES

X509SKI

X509 SK I	5wTucJERkkT5DpKPVkMeBx2/BJw=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Status Starting Time	2020-06-15T22:00:00Z

4.12.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.5734.3.17.5
Description		

4.12.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.12.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.13 - Service (granted): Sellos cualificados de tiempo emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[es]*	*Sellos cualificados de tiempo emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020*
Name	*[en]*	*Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *106110774237859830093543854131413521392*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIXDCCBkSgAwIBAgIQT9QxFrQk7C5e7JYmlZwT8DANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFUzERMA8GA1UECgwIRk5NVC1SQ00xDjAMBgNVBAsMBUNlcmVzMRgwFgYDVQRhDA9WQVRFUy1R
MjgyNjAwNEoxKTAnBgNVBAMMIEFDIFVuaWRhZGVzIGRlIFNlbGxhZG8gZGUgVGllbXBvMBAXDTIw
MDYxOTEwNDAzOFoXDTI1MDYxOTEwNDAzOFowgZgxCzAJBgNVBAYTAkVTMQ8wDQYDVQQHDAZNQURS
SUQxETAPBgNVBAoMCEZOTVQtUkNNMQ4wDAYDVQQLDAVDRVJFUzEYMBYGA1UEYQwPVkFURVMtUT14
MjYwMDRKMTswOQYDVQQDDDJBVVRPUklEQUQgREUgU0VMTEFETyBERSBUSUVNUE8gRk5NVC1SQ00g
LSBUU1UgMjAyMDCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBALkR0QBH5iptiwYdWd4M
m7MnuXYysfCRHo4wjOfysvdsO2xTHGROWLpPepQsGdQUCvedhnarMo27tdlek3u07hEcpxHvPCjqv
tZJahCpHDwB9t4vPVu8QOcOVIGvnXgZ+9hRW62+xBo2yUattGVME7XFNOpEnz97Ml+cyfUq9ZC1j
sJrP31RX4x3tIbPzMgqSgwWT+40t5jLQbo3pvYd6uHuAf24Ncq2zw7iS6ZnyHRwtYUIDIR9v8jbm
68SSEyAbRF6AIyhCfexW7emIydVo3YKyMrcpfvOzHc8WTKnGiAUUnhtjf3XWA5FW+4EtWiqXwiK
dg1qXSlEHKJMvaHGjzMV0Ihp+ZCMpWSpfer1pmvnNxHeJxx+3GV4O06NPluGLsLtMz9SdGZoch+
0FX754PEHK1rv50cqLa00I7ZNSwCyKKC7ZVwre/UrONSxYlUzFjbI5lug1VitxPU9O6KxeNKWlc+
YpoGUqDPpuUQmGfMMBmPE5F1256t1b3cp8xudQIDAQABo4IDQjCCAz4wDAYDVR0TAQH/BAJwADAW
BgNVHSUBAf8EDDAKBggrBgEFBQcDCDAOBgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFPEOd00KMudp
pZAAGuSqFc+7iQDSMB8GA1UdIwQYMBaAFEC5VQSoT39gkO0RISXDJfpu9IXVMIHDBggrBgEFBQcB
AwSBtjCBszAIBgYEAI5GAQEwCwYGBACORgEDAgEPMBMGBgQAjkYBBjAJBgcEAI5GAQYCMG4GBgQA
jkYBBTBkMDAWKmh0dHBzOi8vd3d3LmNlcnQuZm5tdC5lcy9wZHMvUERTX1NUX2VzLnBkZhMCZXMw
MBYqaHR0cHM6Ly93d3cuY2VydC5mbm10LmVzL3Bkcy9QRFNtU1RlZW4uaGRmEwJlbjAVBggrBgEF
BQcLAjAJBgcEAIvsSQECMDkGA1UdIwQyMDAwLqAsoCqGKGh0dHA6Ly93d3cuY2VydC5mbm10LmVz
L2NybHNhY3N0L0NSTC5jcmwwggEVBgNVHSAEggEMMIIBCDCB+gYKKwYBBAGsZgMSATCB6zApBggr
BgEFBQcCARYdaHR0cDowL3d3dy5jZXJ0LmZubXQuZXMvZHBjcy8wgb0GCCsGAQUFBwICMIGwDIGt
Q2VydGlmaWNhZG8gY3VhbGlmaWNhZG8gZGUgc2VsbG8gZWxlY3Ryw7NuaWNvIHBhcmEgVFNVLiBT
dWpldG8gYSBsYXMgY29uZXMgZGUgdXNvIGVdcHVlc3RhcyBlbiBEUEMgZGUgRk5NVC1S
Q0tsIE5JRzogUTI4MjYwMDQtSiAoQy9Kb3JnZSBkdWFudEwNi0yODAwOS1NYWRyaWQhRXNwYcOx
YSkwCQYHBACL7EABATB/BggrBgEFBQcBAQRzMHEwMgYIKwYBBQUHMAKGJmh0dHA6Ly93d3cuY2Vy
dC5mbm10LmVzL2NlcnRzL0FDU1QuY3J0MDsGCCsGAQUFBzABhi9odHRwOi8vb2NzcHN0LmNlcnQu
Zm5tdC5lcy9vY3Nwc3QvT2NzcFJlc3BvbmRlcyArBgNVHRAEJDAigA8yMDIwMDYxOTEwNDAzOFqB
DzIwMjQwNjE5MTA0MDM4WjANBgkqhkiG9w0BAQsFAAOCAgEAsUvE8mRuOx6djDdsqy12o9g8oen
ZwNE1yd4zv4HbA4365NDnLHdkd+KumJnzd8/zSRvBYXKEPqLaYcZzopMDC8pl3TmC/8olPlzbGDK
8Z4eQ6wqKDAUsOyFWShbtPAWySDU6zkJmEDPMuS3kM4GRZHbmG2UK2FTjAUgM2ljGPGAtBMKMq
ZDyD91kEcuyTMN+dv5L5RA+wPGnFdHVKQBmlB3/tj9kmKM05vqiTTzCz9/AvvWmqys5hBclK/i8
HGkydpbAGAp1ZJnm487szEPuGR5Ugly4rI5yMmOJnn3s6KekEDxBL0FgnOtgeqLjTx50mrp2H0
6iHdrXC3E4nEghZFqfiOzJiYyvQ36qml2A5b+Ldv4d342rdwcpdxWoD/IO4xnuWV15zrRZoUunLO
H7SOk3jBdnc2AMGswh9IvruQ9SvUf59UMYBw9fk1zIG1wdcNu7U1m5c05uaBHpyyLjjtw8Gtfil+
0d/mLc1ggjp40r4E/Ag/oqk/tMKT1XCJrUHvkWqOEthoyTA1VXx+EctzM67Wg6R3hTcC/FhEr
Je9cMkgZ32g2GEDEo4CnsDIYNs28USSu4rhn7RUfvOnzz2AorXA0SLG0pbEFyynjz9Bn+ropmX/
4UqV8v6phhjO5BrgBdQIX62HkntnhoVHYgM98WaunXeQGm8k=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *AC Unidades de Sellado de Tiempo*

Issuer 2.5.4.97: *VATES-Q2826004J*

Issuer OU: *Ceres*

Issuer O: *FNMT-RCM*

Issuer C:	*ES*
Subject CN:	*AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020*
Subject 2.5.4.97:	*VATES-Q2826004J*
Subject OU:	*CERES*
Subject O:	*FNMT-RCM*
Subject L:	*MADRID*
Subject C:	*ES*
Valid from:	*Fri Jun 19 12:40:38 CEST 2020*
Valid to:	*Thu Jun 19 12:40:38 CEST 2025*
Public Key:	*30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:B9:11:D1:00:47:E6:2A:6D:8B:06:1D:59:DE:0C:9B:B3:27:B9:76:2F:B2:50:91:1E:8E:30:8D:07:F2:C9:DB:0E:CF:14:C7:19:13:96:2E:93:DE:A5:0B:06:75:05:02:BD:E7:61:89:AA:CC:A3:6E:ED:76:57:A4:DE:ED:3B:84:47:29:C4:7B:CF:0A:3A:AF:B5:92:5A:84:2A:47:0F:00:7D:B7:8B:CF:56:EF:10:39:E3:95:94:6B:E7:5E:06:7E:F6:14:56:EB:6F:B1:06:8D:B2:51:AB:6D:19:53:04:ED:71:4D:3A:91:27:CF:DE:CC:97:E7:B2:7D:4A:BD:64:2D:63:B0:9A:CF:DF:54:57:E3:1D:ED:7D:B3:F3:32:0A:92:83:05:93:FB:8D:2D:E6:32:D0:6E:8D:E9:BD:87:7A:B8:7B:80:7F:6E:0D:72:AD:B3:C3:B8:92:E9:99:F2:1D:1C:1F:61:42:03:7D:1F:6F:F2:36:E6:EB:CE:52:13:20:1B:44:5E:80:23:28:42:7D:EC:56:ED:E9:88:C9:D5:68:DD:82:B2:32:B7:29:7E:F3:B3:1D:CF:16:4C:AA:E2:1A:20:14:52:78:6D:8D:FD:D7:58:0E:45:5B:EE:04:B5:68:AA:5F:08:8A:76:0D:6A:5D:29:44:1C:A2:49:32:F6:87:1A:3C:CC:57:40:E9:F9:90:8C:A5:64:A9:27:2A:F5:A6:7B:E7:37:11:DE:27:1C:7E:E4:65:78:3B:4E:8D:3E:5B:86:2E:C2:ED:33:FC:FD:49:D1:99:A1:C8:7E:D0:55:FB:E7:83:C4:1C:AD:6B:BF:9D:1C:A8:B6:B4:D0:8E:D9:35:2C:02:C8:A2:82:ED:95:70:AD:EF:D4:AC:E3:52:C5:89:54:CC:58:DB:97:92:2E:83:55:62:B7:13:D4:F4:EE:8A:C5:E3:4A:5A:57:BE:62:9A:06:52:A0:CF:A6:E5:10:98:67:CC:30:19:8F:13:91:65:DB:9E:AD:D5:BD:DC:A7:CC:6E:75:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*F1:0E:77:4D:0A:32:E7:69:A5:90:00:1A:E4:A0:15:CF:BB:89:00:D2*
Authority Key Identifier	*40:B9:55:04:A8:4F:7F:60:90:ED:11:95:25:C3:25:FA:5A:F4:85:D5*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
CRL Distribution Points	*http://www.cert.fnmt.es/crlsacst/CRL.crl*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.5734.3.18.1* *CPS pointer: http://www.cert.fnmt.es/dpcs/* *CPS text: [Certificado cualificado de sello electrónico para TSU. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)]* *Policy OID: 0.4.0.194112.1.1*
Authority Info Access	*http://www.cert.fnmt.es/certs/ACST.crt* *http://ocspst.cert.fnmt.es/ocspst/OcspResponder*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*88:15:87:C2:7E:44:DC:07:DA:A3:92:D2:5B:CC:81:38:53:F2:03:63:46:31:65:86:86:87:EE:BC:DB:71:D7:55*

X509SubjectName

Subject CN:	*AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020*
Subject 2.5.4.97:	*VATES-Q2826004J*
Subject OU:	*CERES*
Subject O:	*FNMT-RCM*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*8Q53TQoy52mlkAAa5KAVz7uJANI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-07-28T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5 - TSP: Consorci Administració Oberta de Catalunya - CAOC

.

TSP Name

Name	*[en]*	*Consorci Administració Oberta de Catalunya - CAOC*
Name	*[es]*	*Consorci Administració Oberta de Catalunya - CAOC*

TSP Trade Name

Name	*[en]*	*VATES-Q0801175A*
Name	*[en]*	*Consorci AOC (CATCert)*
Name	*[es]*	*Consorci AOC (CATCert)*
Name	*[en]*	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Name	*[es]*	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Name	*[en]*	*CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

PostalAddress

Street Address	*[en]*	*Via Laietana, 26*
Locality	*[en]*	*Barcelona*
State Or Province	*[en]*	*Barcelona*
Postal Code	*[en]*	*08003*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Via Laietana, 26*
Locality	*[es]*	*Barcelona*
State Or Province	*[es]*	*Barcelona*
Postal Code	*[es]*	*08003*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.aoc.cat*

URI	*[en]*	*mailto:info@aoc.cat*

TSP Information URI

URI	*[en]*	*http://www.aoc.cat*
URI	*[es]*	*http://www.aoc.cat*

5.1 - Service (withdrawn): Qualified certificates issued by CA IdCAT

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by CA IdCAT*
Name	*[es]*	*Certificados Reconocidos emitidos por CA idCAT*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149207157159073437715447019610265252046*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHsDCCBpigAwIBAgIQcEBA0P3KPBk/ojwnYepwzjANBgkqhkiG9w0BAQUFADCB8zELMAkGA1UE
BhMCRVMxOzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2lvIChOSUYgUS0w
ODAxMTc2LUkpMSgwJgYDVQQLEx9TZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvMTUwMwYD
VQQLEyxWZWdldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UE
CxMsSmVyYXJxdWlhIEVudGl0YXRzIGRlIENlcnRpZmljYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMT
BkVDLUFDQzAeFw0wMzEwMzExMDQwMzlaFw0xOTEwMzExMDQwMzlaMIIBMTELMAkGA1UEBhMCRVMx
OzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2lvIChOSUYgUS0wODAxMTc2
LUkpMTQwMgYDVQQHEytQYXNzYXRnZSBkZSBsYSBDb25jZXBjaWkgMTEgMDgwMDgzQmFyY2Vsb25h
MS4wLAYDVQQLEyVTZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvIEVDV0dyMTUwMwYDVQQL
EyxWZWdldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJDSUMtMiAoYykwMzE1MDMGA1UECxMs
RW50aXRhdCBwdWJsaWNhIGRlIGNlcnRpZmljYWNpbyBkZSBjaXV0YWRhbnMxETAPBgNVBAMTCEVD
LUIEQ2F0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu99Aw9QcEXkizypUs83y67eE
RM1LSEGcAUcA0ecGAYDFpya7Ka6p76vsXY0JpXcDydLY5V1ZKC2PsVJWNtBMtrRczAPtX59p1cbH
kCcXv/ImACXjTUlkIOppy4C2jvQA9/0Nmag8PgSCnk+47msKIqncl/p74fQI8kyoucjJPF5ffYvA
dgrSoLA6GDGIG+0maN0x+ydDVMqfphcO7GXnuv9FALEbZfnseq7FpkoXM830UlnxA63GAEmPeSs
0S1JEW6lbk2zRsPuJMX2h99Xyf+lUnpDzP6INWftEP4g1S0smb6JHFBBxTIrXI36UQJkas5hROD
7XhCm2WzkKvrWQJDAQAJBo4IC7TCCAwkwHQYDVR0SBBYwFIESZWNiYWNjQGNhdGNlcnQubmV0MB8G
A1UdEQQYMBaBFGVjX2lkY2F0QGNhdGNlcnQubmV0MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0P
AQH/BAQDAgEGMB0GA1UdDgQWBBTNksBFRjR2DdL0W6J0HavPbLYLuTCCATEGA1UdIwSCASgwggEk
gBSgw4tEqzlRb+XgFrR8Xiim÷IdjaGB+aSB9jCB8zELMAkGA1UEBhMCRVMxOzASBgNVBAoTMkFn
ZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2lvIChOSUYgUS0wODAxMTc2LUkpMSgwJgYDVQQL
Ex9TZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvMTUwMwYDVQQLEyxWZWdldSBodHRwczov
L3d3dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UECxMsSmVyYXJxdWlhIEVudGl0
YXRzIGRlIENlcnRpZmljYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMTBkVDLUFDQ4IQ7is969Qh3hSo
YqwE893EATCB2gYDVR0gBIHSMIHPMIHMBgsrBgEEAVAAQMBDDCBvDAsBggrBgEFBQcCARYgaHR0
cHM6L y93dCaY2F0YzYvqlC3uXQwdmVyQ0lDL TlwgYsGCCsGAQUFBwICMI8aTlTxdWVzdCBzZX10
aWZpY2F0IHOSZW1ldCDebmljYSBpIGV4Y2x1c2l2YW1lbnQgYSBFbnRpdGF0cyBkZSBDZXJ0aWZp
Y2FjatMgZGUgQ2xhc3NlIDIuIFZlZ2V11Gh0dHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlckNJQy0y
MGlGA1UdHwRbMFkwV6BVoFOGI2hd0dHA6L y9lcHNvjZC5jYXRjZXJ0Lm5ldC9jcmwvZWMtYWNjLmNy
blYoaHR0cDovL2Vwc2NkMi5jYXRjZXJ0Lm5ldC9jcmwvZWMtYWNjLmNybDANBgkqhkiG9w0BAQUF
AAOCAQEAGUdf7hMDZziT9HLVyezsEJHI4KazVHUNRuyrxWsUTPDBHwOOO6KtAElKbyxKwh8SX+n
JwIGVZXwYgZXSu0zyJp3v+pcXwSrRPmovsD7C8JsyrJnaMw7zqTz55Rc8GBEyoznflRkl3MiNONV
iLDrI30G+JN/gwExVFA9n/3noXR2Hmi+FqlE/btZ+xoT1QJGbgjH3qAg7DbAYh2DOQ2Dy9F5i5/
Y5KXwEypcsNq7j8duwFGcBEUlrV2JdqKbc76sKulC3rtSo6NpodkZPRbdKn10+xcpp91I58tgBNW
ZRTxPVig0JvRAudFQCxY4PF5WSWqz7GaMUm2Nhqw8jpmNA==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-ACC*

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu https://www.catcert.net/verarrel (c)03*

Issuer OU:	*Serveis Publics de Certificacio*
Issuer O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Issuer C:	*ES*
Subject CN:	*EC-IDCat*
Subject OU:	*Entitat publica de certificacio de ciutadans*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*
Valid from:	*Fri Oct 31 11:40:39 CET 2003*
Valid to:	*Thu Oct 31 11:40:39 CET 2019*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BB:DF:40:C3:D4:1C:11:79:22:CF:2A:54:B3:CD:F2:EB:B7:84:44:CD:4B:48:41:9E:01:47:80:D1:E1:80:60:31:69:C9:AE:ED:29:AE:A9:EF:AB:D7:60:ED:29:5D:C0:F2:74:B5:79:57:56:4A:0B:33:EC:B5:52:56:34:10:4C:B6:B0:5C:CC:03:C8:5F:9F:69:D5:C6:C7:90:27:17:BF:F2:26:00:25:E3:4D:42:24:20:EA:69:CB:80:B6:8E:F4:00:F7:FD:0D:99:A8:3C:3E:04:82:9E:4F:B8:EE:6B:0A:22:A9:DC:97:FA:7B:E1:F4:08:F2:4C:AB:B9:C8:C9:3C:5E:5F:7D:8B:C0:76:0A:D2:A0:B0:3A:1B:31:88:1B:ED:26:68:DD:31:FB:27:43:54:CA:9F:A6:17:8E:EC:65:E7:BA:FF:45:00:B1:1B:65:F9:EC:7A:AE:C5:A6:4A:17:33:CD:F4:6D:49:67:C4:0E:B7:18:01:26:3D:E4:AC:D1:2D:49:11:6E:A5:86:4D:B3:46:C3:EE:24:C5:F6:87:DF:57:C9:FF:A5:52:7A:43:CC:FE:88:35:67:ED:10:FE:20:D5:2D:2C:99:BE:89:1C:50:41:C5:32:2B:5C:8D:FA:51:02:64:6A:CE:61:7D:13:83:ED:78:42:9B:FD:96:AC:AB:EB:59:02:03:01:00:01*
Issuer Alternative Name	*ec_acc@catcert.net*
Subject Alternative Name	*ec_idcat@catcert.net*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*CD:92:C0:45:46:34:76:0D:D2:F4:5B:A2:74:1D:AB:CF:6C:B6:0B:B9*
Authority Key Identifier	*A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12* *CPS pointer: https://www.catcert.net/verCIC-2* *CPS text: [Aquest certificat semet única i exclusivament a Entitats de Certificació de Classe 2. Vegeu https://www.catcert.net/verCIC-2]*
CRL Distribution Points	*http://epscd.catcert.net/crl/ec-acc.crl* *http://epscd2.catcert.net/crl/ec-acc.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*95:4B:88:92:23:49:8A:ED:51:AA:7A:29:B6:2E:ED:24:BE:03:CD:48:1D:18:2E:03:EB:83:BA:E8:DD:7B:D7:1B*

X509SubjectName

Subject CN:	*EC-IDCat*
Subject OU:	*Entitat publica de certificacio de ciutadans*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2018-03-15T01:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA IdCAT*
Name	*[es]*	*Certificados Reconocidos emitidos por CA idCAT*

Service digital identities

X509SubjectName

Subject CN:	*EC-IDCat*
Subject OU:	*Entitat publica de certificacio de ciutadans*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*zZLARUY0dg3S9FuidB2rz2y2C7k=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

5.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA IdCAT*
Name	*[es]*	*Certificados Reconocidos emitidos por CA idCAT*

Service digital identities

X509SubjectName

Subject CN:	*EC-IDCat*
Subject OU:	*Entitat publica de certificacio de ciutadans*

Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*zZLARUY0dg3S9FuidB2rz2y2C7k=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2006-01-23T00:00:00Z*

5.2 - Service (withdrawn): Certificados Reconocidos emitidos por CA AL

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA AL*
Name	*[en]*	*Qualified certificates issued by CA AL*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*81871235804792199700514938710945526542*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHgzCCBmugAwIBAgIQPZTTkwQ5Yio+HE2mvtFzDjANBgkqhkiG9w0BAQUFADCB8zELMAkGA1UE
BhMCRVMxOzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VyZGlmaWNhY2hlICBOSUYgUS0w
ODAxMTc2LUkpMSgwJgYDVQQLEx9TZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvMTUwMwYD
VQQLEyxWZWldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UE
CxMsSmVyYXJxdWlhIEVudGl0YXRzIGRlIENlcnRpZmlqYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMT
BkVDLUFDQzAeFw0wMzAxMDgxNjExMTIwFw0xOTAxMDcyMjU5NTIaMIBBjEiLMAkGA1UEBhMCRVMx
OzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VyZGlmaWNhY2lvIC0OSUYgUS0wODAxMTc2
LUkpMTQwMgYDVQQHEytQYXNzYXRnZSBkZSBsYSBlb25jZXBjaWlgMTEgMDgwMDggQmFyY2Vsb25h
MS4wLAYDVQQLEyVTZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvIEVDV0yMTYwNAYDVQQL
Ey1WZWldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJDSUMtMiAgKGMpMDMxLDAqBgNVBAsT
I0FkbWIuaXNkcmFjaW9uczvBMb2NlbHMgZGUgQ2F0YWx1bnlhMQ4wDAYDVQQDEwVFQy1BTDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJoUgFs1ryKFTrtMqUBvSSBenITsbo89bowr9WN
yPsngblkMpay80EY7pAbDIT6aW+Glre2e+FEKAycrJ95aB/lXI8E65XlSZxGIsvlPjY6WcQ/bMeA
m9tr0j7fMFGew47kCPLXIEt75tkhx2JpnFuXXdQIVVzS3zbWc9CKoA6hqxzlkg3LRCyhQ5x7PC
knNlaJN3y+Nk+Wd+YWrsd+wC+VUz10uEwcSIMZJa1bWNq9Lzxc+r6XJOY6E7k4AGqfsHdcoyP6j
SPkUdCZv84SNN/TMyL2y+8u4dp06TUdC0Yy3zEcht7/AHu/0CH+YR8XGiPL+0JpuygaUBhD0TYMC
AwEAAaOCAtswggLXMB0GA1UdEgQWMBSBEmVjX2FjY0BjYXRjZXJ0Lm5ldDAPBgNVHRMBAf8EBTAD
AQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUTOyNSdQrAgOa0EgwCktrvTF6pjQwggExBgNV
HSMEggEoMIIBJIAUoMOLRKo5pUWi4Ba0lF4opnpXY2hgfmkgfYwgfMxCzAJBgNVBAYTAkVTMTsw
OQYDVQQKEzJBZ2VuY2lhIENhdGFsYW5hIGRlIENlcnRpZmlqYWNpbyAoTklGIFEtMDgwMTE3Ni1J
KTEoMCYGA1UECxMfU2VydmVpcyBQdWJsaWNzIGRlIENlcnRpZmlqYWNpbzE1MDMGA1UECxMsVmVn
ZXUgaHR0cHM6Ly93d3cuY2F0Y2VydC5uZXQvdmVyYXJyZWwgKGMpMDMxNTAzBgNVBAsTLEplcmFy
cXVpYSBFbnRpdGFlcyBkZSBlZXJhcnF1aWZpY2FjaW8gQ2F0YWxhbmVzMQ8wDQYDVQQDEwZFQy1BQ0OC
EOArPevUJd4UgGKsBPPdxAEwgdwGA1UdIASB1DCB0TCBzgYLKwYBBAH1eAEDAQwwgb4wLAYIKwYB
BQUHAgEWIGh0dHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlckNJQy0yMIGNBggrBgEFBQcCAjCBgBp+
QXF1ZXN0IGNlcnRpZmlqYXQg6XMgZW3ocyD6bmljYSBplGV4Y2x1c2l2YWIlbnQgYSBFbnRpdGF0
cyBkZSBDZXJlIaWZpY2FjaMgZGUgQ2xhc3NlIDIuIFZlZ2V1IGhtdHBzOi8vd3d3LmNhdGNlcnQu
bmV0L3ZlckNJQy0yMGIGA1UdfwRbMFkwV6BVoFOGJ2h0dHA6Ly9lcHNjZC5jYXRjZXI0Lm5ldC9j
cmwvZWMtYWNjLmNybYloAHR0cDovL2Vwc2NkMi5jYXRjZXJ0Lm5ldC9jcmwvZWMtYWNjLmNybDAN
BgkqhkiG9w0BAQUFAAOCAQEAnnbeofQKiDCDVaWjhA1yMutbVA005Qlc1ezf9BUJhj T02b7556EE
LX4Oa7TTXVVE9CL0NCXfSdTBjmE/9Ls2XSPXvXlYuVR86V0gXBVdeCGkynYzymXPdgASVZTIoh3n
nSxOttzby71/6Rj+4CNBAFysLNYu2nIMSPJarXIl3Xzd1KFdJuAKAKX13Q45uZVc+W7suYDKvqN
rdBo0Fhda1G8b7xs58HGRFU2vAKmHsSORWxLwaIuOjkK010bpO5tKeLG4dSebteIUwQ2GeyELc2F
GuOJgKHtWOWncSkOtRHh9aowyXSmGo9uwbOssJYQL9X0k4dY/U0K/Kea8Ua1RA==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-ACC*

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu https://www.catcert.net/verarrel (c)03*

Issuer OU: *Serveis Publics de Certificacio*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-AL*

Subject OU: *Administracions Locals de Catalunya*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Valid from: *Wed Jan 08 17:11:18 CET 2003*

Valid to: *Mon Jan 07 23:59:59 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9A:14:80:5B:35:AF:22:85:4E:B7:CC:A9:FF:C1:BD:24:81:7A:72:13:B1:BA:3C:F7:AA:30:AF:D5:8D:C8:FB:27:81:B
9:64:32:96:B2:F3:41:18:EE:90:1B:0C:84:FA:69:6F:86:96:B7:B6:7B:E1:44:28:0C:9C:AC:9F:79:68:1F:E5:5C:8F:04:EB:95:E5:49:9C:46:22:CB:E5:3E:36:3A:59:C4:3F:6C:C7:80:9B:DB:6B:D3:48:FB:7C:C1:46:7B:0E:3B:90:2
3:CB:5C:81:2D:EF:9B:64:87:1D:A5:8E:71:6E:5D:77:50:21:55:73:4B:78:B3:6D:67:3D:08:AA:00:EA:1A:B1:CE:59:20:DC:B4:42:CA:14:39:C7:B3:C2:92:73:48:68:93:77:CB:E3:7C:F9:67:7E:61:6A:EC:77:EC:02:F9:55:33:D6
:2D:2E:13:07:B7:7C:C6:49:6B:56:D6:36:AF:4B:CF:17:3E:AF:A5:C9:39:8E:84:EE:4E:00:1A:A7:EC:1D:D7:A8:C8:FE:A3:48:F9:14:74:26:6F:F3:84:8D:37:F4:CC:C8:BD:B2:FB:CB:B8:76:9D:3A:4D:47:42:D1:8C:B7:CC:47:
21:B7:BF:C0:1E:EF:F4:08:7F:98:47:C5:C6:88:F2:FE:D0:9A:6E:CA:06:94:06:10:F4:4D:83:02:03:01:00:01

Issuer Alternative Name *ec_acc@catcert.net*

Basic Constraints *IsCA: true*

Subject Key Identifier	*4C:EC:8D:49:D4:2B:02:03:9A:D0:48:30:0A:4B:6B:BD:31:7A:A6:34*
Authority Key Identifier	*A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12* *CPS pointer: https://www.catcert.net/verCIC-2* *CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu https://www.catcert.net/verCIC-2]*
CRL Distribution Points	*http://epscd.catcert.net/crl/ec-acc.crl* *http://epscd2.catcert.net/crl/ec-acc.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*59:2C:50:8E:39:D7:66:5F:84:45:86:C3:B9:E7:65:AF:D5:D8:0B:BE:05:F9:28:9C:B0:DE:D5:71:1A:C9:C1:0A*

X509SubjectName

Subject CN:	*EC-AL*
Subject OU:	*Administracions Locals de Catalunya*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-03-15T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA AL*
Name	*[en]*	*Qualified certificates issued by CA AL*

Service digital identities

X509SubjectName

Subject CN:	*EC-AL*
Subject OU:	*Administracions Locals de Catalunya*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *TOyNSdQrAgOa0EgwCktrvTF6pjQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA AL*
Name	*[en]*	*Qualified certificates issued by CA AL*

Service digital identities

X509SubjectName

Subject CN:	*EC-AL*
Subject OU:	*Administracions Locals de Catalunya*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*TOyNSdQrAgOa0EgwCktrvTF6pjQ=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2010-05-05T00:00:00Z*

5.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.3 - Service (withdrawn): Certificados Reconocidos emitidos por CA SAFP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por CA SAFP*

Name *[en]* *Qualified certificates issued by CA SAFP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *148786221414740922626357724534625015094*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHrTCCBpWgAwIBAgIQb+8xFPRPzN8+HCEWmIwVNjANBgkqhkiG9w0BAQUFADCB6TELMAkGA1UE
BhMCRVMxOzA5BgNVBAo7MkFnZWS5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2lvICBOSUYgLUSbw
ODAxMTc2LUkpMS4wLAYDVQQLEyVTZXJ2ZWIzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvIEVDVi0x
MTYwNAYDVQQLEy1WZWdldSBodHRwczovL3d3dy5jYXRjZXJ0LmS5ldC92ZXJDSUMtMSAgKGMpMDMx
ITAfBgNVBAsTGEdlbmVyYWxpdGF0IGRlIENhdGFsdW55YTESMBEGA1UEAxMJRUMtR0VOQ0FUMB4X
DTAzMDEwODEzMDExMFoXDTE5MDEwNzIyNTk1OVowggExMQswCQYDVQQGEwJFUzE7MDkGA1UEChMy
QWdlbmNpYSBDYXRhbGFuYSBkZSBDZXJ0aWZpY2FjaW8gKE5JRiBRLTA4MDExNzYtSSkxNDAyBgNV
BAcTK1Bhc3NhdGdlIGRlIGxhIENvbmNlcGNpbyAxMSAwODAwOCBCYXJjZWxvbmExLjAsBgNVBAsT
JVNlcnZlaXMgUHVibGljcyBkZSBDZXJ0aWZpY2FjaW8gRUNWLTIxNzA1BgNVBAsTLlZlZ2V1Igh0
dHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlckNJQy0yICAgKGMpMDMxNDAyBgNVBAsTK1NlY3IdGFy
aWEgZCdBZG1pbmlzdHJlbY2lvIGkgRnVuY2lvIFB1YmxpY2ExEDAOBgNVBAMTB0VDLVNBRlAwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCZl8bKC2Eu/8GGZGTUSddbm3ZmMAUuq/N5CKN
Hyw0FpeBE1GwkPvUhg4b9+2PG56NlLP8GF/0CAIO4520J/hlCXFzY6/91K7SDpY0Cg1TITnpK9wk+
wH/+kvkj2yWQ0bxb8tGZO356mhP8KVLWaXFERhkswkRb7lOQoal/afmEJOflloC1L91/99eM5FTsP
0hE8R2int/ezgie7wKWuXHCdjtdNk9dR21AUFHj3+HH4LcF8X6qfzc3VcDrY0ZQzgk8rkMmQMRu
fc6eH6zOKFbngSys1VMwQFhhlRjHWqh59CpxhhWoH9JGE2xYOm1CmSFmzhMTglv5vPKJo2DWG4aJ
AgMBAAGjggMEMIIDADAgBgNVHREGTAXgRVIY19nZW5jYXRAY2F0Y2VydC5uZXQwHgYDVR0RBBcw
FYETZWNfc2FmcEBjYXRjZXJ0LmS1dDAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAd
BgNVHQ4EFgQUBbflTxZS3frmksCicnlWYFTCIBMwggExBgNVHSMEggEoMIIBJIAUMWpcCkZONo9C
47BgKwwPLS+T3xShgfmkgfYwgfMxCzAJBgNVBAYTAkVTMTswOQYDVQQKEzJBZ2VuY2lhIENhdGFs
YW5hIGRlIENlcnRpZmljYWNpbyAoTklGIFEtMDgwMTE3N1JKTEoMCYGA1UECxMfU2VydmVpcyBQ
dWJsaWNzIGRlIENlcnRpZmljYWNpbzE1MDMGA1UECMsVmVnZXUgaHR0cHM6Ly93d3cuY2F0Y2Vy
dC5uZXQvdmVyYXJyZWwgKGMpMDMxNTAzBgNVBAsTLipkcmFycXVpYSBFbnRpdGF0cyBkZSBDZXJ0
aWZpY2FjaW8gQ2F0YWxhbmVzMQ8wDQYDVQQDEwZFQy1BQ0OCECC9PeBpBD0lPhwLnIJS9ClwgdwG
A1UdIASB1DCB0TCBzgYLKwYBBAH1eAEDAQwwgb4wLAYIKwYBBQUHAgEWIGh0dHBzOi8vd3d3LmNh
dGNlcnQubmV0L3ZlckNJQy0yMiGNBggrBgEFBQcCAjCBgBp+QXF1ZXN0IGNlcnRpZmljYXQg6XMg
ZW3ocyD6bmljYSBpGVdY2x1c2I2YW1lbnQgYSBFbnRpdGFlcyBkZSBDZXJ0aWZpY2FjaMgZcUg
Q2xhc3NlIDluIFZlZ2V1IGh0dHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlckNJQy0yMGgGA1UdFwRh
MF8wXaBboFmGKmh0dHA6Ly9lcHNjZC5jYXRjZXJ0LmS1dC9jcmwvZWMtZ2VuY2F0LmNybIYraHR0
cDovL2Vwc2NkMi5jYXRjZXJ0LmS1dC9jcmwvZWMtZ2VuY2F0LmNybDANBgkqhkiG9w0BAQUFAAOC
AQEAeZLc3+HSKjopRiwYDxDc/r2B9zmI/pamjMcYCq3ffDBKnIPmn1wWGVdeQ+sxdzLWpjZxK2v8r
fnBpo55YmRISo3GSlCrx35p9eLeawtRZ0HOAAhC36VIDKUgcGFB0GIFlI7Xy/9saAIIDcAKykvd
855tss6vyNpHo06GRFpoyhMuirq62HCGVKFn56Cf2K51pZmsr3asKQ3TU8p/cOvERw245QIfyAMf
2R8cGIl4+lHRP0/tu5Icya19a5SAaFu6Q/aNcKEqYMKvKmqZGy5+e1p+7eS5hQUlwtDFVBlGDhHB
aZgOtxNUIzFBePCCnulaWRIrHn4gAt1jcwxWPPvJg==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-GENCAT*

Issuer OU: *Generalitat de Catalunya*

Issuer OU: *Vegeu https://www.catcert.net/verCIC-1 (c)03*

Issuer OU:	*Serveis Publics de Certificacio ECV-1*
Issuer O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Issuer C:	*ES*
Subject CN:	*EC-SAFP*
Subject OU:	*Secretaria d'Administracio i Funcio Publica*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*
Valid from:	*Wed Jan 08 14:01:10 CET 2003*
Valid to:	*Mon Jan 07 23:59:59 CET 2019*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:99:23:C6:CA:0B:61:2E:FF:C1:86:64:64:D4:49:D7:5B:9B:76:66:30:09:49:BA:AF:CD:E4:22:8D:1F:2C:34:16:97:81:13:51:B0:90:FB:D4:86:0E:21:F7:ED:8F:1B:9E:8D:94:B3:FC:A0:5F:F4:08:09:4E:E3:9D:8E:27:F8:48:09:71:73:63:AF:FD:D4:AE:D2:0E:96:34:0A:04:C8:4E:7A:4A:F7:09:3E:C0:7F:FE:92:F9:23:DB:25:90:D1:BC:5B:F2:D1:99:3B:9E:A6:84:FF:0A:54:B5:9A:5C:51:11:86:4B:30:91:16:FB:20:E4:28:6A:5F:DA:7E:61:09:39:F9:5F:A0:2D:4B:F7:5F:FD:F5:E3:39:15:3B:0F:D2:11:3C:47:68:A7:B7:F8:9C:82:37:BB:C0:A5:AE:5C:70:9D:8A:37:4D:93:D7:51:DB:50:14:14:78:F7:F9:F7:C7:E0:B7:05:F1:7E:AA:23:37:37:55:E0:EB:63:46:50:CE:09:3C:AE:43:26:40:C4:6E:7D:CE:9E:1F:AC:CE:28:56:E7:81:2C:AC:D5:53:30:40:58:61:95:18:C7:5A:A8:79:F4:2A:71:86:15:A8:1F:D2:46:13:6C:58:3A:6D:42:99:21:66:CE:13:13:80:8B:F9:BC:F2:89:A3:60:D6:1B:86:89:02:03:01:00:01*
Issuer Alternative Name	*ec_gencat@catcert.net*
Subject Alternative Name	*ec_safp@catcert.net*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*05:B7:ED:4F:16:52:DD:FA:E6:92:C0:A2:72:79:56:60:54:C2:24:13*
Authority Key Identifier	*31:6A:5C:0A:46:4E:37:AF:42:E3:B0:60:2B:0C:0F:2D:2F:93:DF:14*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12* *CPS pointer: https://www.catcert.net/verCIC-2* *CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu https://www.catcert.net/verCIC-2]*
CRL Distribution Points	*http://epscd.catcert.net/crl/ec-gencat.crl* *http://epscd2.catcert.net/crl/ec-gencat.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*20:7C:EC:E0:38:B9:82:6A:12:0A:91:9D:4B:41:BC:A8:F3:7F:2E:99:46:21:BF:5A:99:3A:04:08:7D:55:6D:C6*

X509SubjectName

Subject CN:	*EC-SAFP*
Subject OU:	*Secretaria d'Administracio i Funcio Publica*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-03-15T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA SAFP*
Name	*[en]*	*Qualified certificates issued by CA SAFP*

Service digital identities

X509SubjectName

Subject CN:	*EC-SAFP*
Subject OU:	*Secretaria d'Administracio i Funcio Publica*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*BbftTxZS3frmksCicnlWYFTCJBM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por CA SAFP*

Name *[en]* *Qualified certificates issued by CA SAFP*

Service digital identities

X509SubjectName

Subject CN: *EC-SAFP*

Subject OU: *Secretaria d'Administracio i Funcio Publica*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *BbftTxZS3frmksCicnlWYFTCJBM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.4 - Service (withdrawn): Certificados Reconocidos emitidos por CA PARLAMENT

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por CA PARLAMENT*

Name *[en]* *Qualified certificates issued by CA PARLAMENT*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *499210838242904253819539411378428836 17*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHmzCCBoOgAwIBAgIQJY5zdgD/mG9A4oB/uzdSwTANBgkqhkiG9w0BAQUFADCB8zELMAkGA1UE
BhMCRVMxOzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2lvIChOSUYgUS0w
ODAxMTc2LUkpMSgwJgYDVQQLEx9TZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvMTUwMwYD
VQQLEyxWZWldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UE
CxMsSmVyYXJxdWlhIEVudGl0YXRzIGRlENlcnRpZmljYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMT
BkVDLUFDQzAcFw0wNDA2MzAwODU3MzVaFw0yMDA2MjkyMTU5NTlaMIIBGTELMAkGA1UEBhMCRVMx
OzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2lvIChOSUYgUS0wODAxMTc2
LUkpMTQwMgYDVQQHEytQYXNzYXRnZSBkZSBsYSBDb25jZXBjaW8gMTEgMDgwMDggQmFyY2Vsb25h
MSgwJgYDVQQLEx9TZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2lvMTUwMwYDVQQLEyxWZWdl
dSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJDSUMtMzAoYykwMzEzMB0GA1UECxMWUGFybGFt
ZW50IGRlIENhdGFsdW55YTEVMBMGA1UEAxMMRUMtUEFSTEFNRU5UMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAvAmX1wfedLan9F/PnJ5xlSlily+SNnUMnLac2BHr2qbl7HurjXXwtbl8
BRZMjz9gudNd5ahQRwSao0EayZ6y7X5emDfkwtaIoW2+9OshZLXXynwuxJLJJkLQCSQdFborJQVc
Tr64H6ooH2k7jt6rXLc0fGfz3VgK/1y6m774X6VE/XZnGOgbBCmKfytm140AgR1uc55NGYrcEkBa
cAzCxYEsiTC+D9fNwfs9rvZTdND+xcFudNZRXZENczXM/B554kHCwRBAApbCTrOta1hnCwe75Q
+SJhm/ynGj4441T7P9Bij7QvRARvxC3cO5ZfHQ17Ualb646rYodOoTma7wIDAQABo4IDADCCAvww
HQYDVR0SBBYwFIESZWNfYWNjQGNhdGNlcnQubmV0MCMGA1UdEQQcMBqBGGVjLXBhcmxhbWVudEBj
YXRjZXJ0Lm5ldDAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUHhOY
6sfCWVW23i8+ypv/6ssuLBQwggExBgNVHSMEggEoMIIBIJAUoMOLRKo3pUW/bHBa0IF4qmvpX Y2h
gfmkgfYwgfMxCzAJBgNVBAYTAkVTMTswOQYDVQQKEzJBZ2VuY2lhIENhdGFsYWShIGRlIENlcnRp
ZmljYWNpbyAoYklGIFEtMDgwMTE3Ni1JKTEoMCYGA1UECxMfU2VydmVpcyBQdWJsaWNzIGRlIEN1
cnRpZmljYWNpbzE1MDMGA1UECxMsVmVnZXUgaHR0cHM6Ly93d3cuY2F0Y2VydC5uZXQvdmVyYXJy
ZWwgKGMpMDMxNTAzIBgNVBAsTLEplcmFyeXVpYSBFbnRpdGF0cyBkZSBDZXJ0aWZpY2FjaW8gQ2F0
YWxhbmVzMQ8wDQYDVQQDEwZFQy1BQ0OCEO4rPevUld4UqGKsBPPdxAEwgdwGA1UdIASB1DCB0TCB
zgYLKwYBBAH1eAEDAQwwgb4wLAYIKwYBBQUHAgEWIGh0dHBzOi8vd3d3LmNhdGNlcnQubmV0L3Zl
ckNJQy0yMIGNBggrBgEFBQcCAjCBgBp+QXF1ZXN0IGNlcnRpZmljYXQg6XMgZW3ocyD6bmljYSBp
IGV4Y2x1c2l2YW1lbnQgYSBFbnRpdGF0cyBkZSBDZXJ0aWZpY2FjaMgZGUgQ2xhc3NlIDIuIFZl
Z2V1lGh0dHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlckNJQy0yMGIGA1UdHwRbMFkwV6BVoFOGJ2h0
dHA6Ly9lcHNjZC5jYXRjZXJ0Lm5ldC9jcmwvZWMtYWNjLmNybDANBgkqhkiG9w0BAQUFAAOCAQEAfv+hU/kx0SF8LpensM9+
ZV1Ml+Ovq8dGpV9Pf6v+a+t8iPYz1i1OlmUkWQcxOmA2O+n/YZ0kY3X+4Wdx4jboRbrqSQzG
PEwTWpnrdhJl2wAu9wwtisWw+29YnGllmsC3oOuaCnwr+WJ+zmHMuAxmh1e20bMIGXva1HyjL q4
lPGsmDN9Ljv+pefI0/Kcr3fbl+cJJXlDGib+ZES/SrkMvrQ/qQWfrOkHJHaMdbC0Cprd0qJOnFB4
xNxm5Zj3V8nIlSdiOBrQjckdRr6GDD4idDQ5xG7dqRfiGJ91pEHi/WZmMvWQd6lRfVYFBBTLzxbg
VD9iz/CZA4IMMnpBjw==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-ACC*

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu https://www.catcert.net/verarrel (c)03*

Issuer OU: *Serveis Publics de Certificacio*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-PARLAMENT*

Subject OU: *Parlament de Catalunya*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*
Valid from:	*Wed Jun 30 10:57:35 CEST 2004*
Valid to:	*Mon Jun 29 23:59:59 CEST 2020*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:09:97:D7:07:DE:74:B6:A7:F4:5F:CF:9C:9E:71:95:22:62:97:2F:92:36:75:0C:9C:B6:9C:D8:11:EB:DA:A6:E5:EC:7B:AB:8D:75:F0:B5:B9:7C:05:16:4C:8F:3F:60:B9:D3:5D:E5:A6:D0:47:04:9A:A3:41:1A:C9:9E:B2:ED:7E:5E:98:37:F1:C2:D6:88:A1:6D:BE:F4:EB:21:64:B5:D7:CA:7C:2E:C4:92:C9:26:42:D0:09:24:1D:15:BA:2B:25:05:5C:4E:BE:B8:1F:AA:28:1F:69:3B:8E:DF:2B:5C:B7:34:14:67:F3:DD:58:0A:FF:5C:BA:9B:BE:F8:5F:A5:44:FD:76:67:18:E8:1B:04:29:8A:7F:2B:66:D7:8D:00:81:1D:6E:73:9E:4D:19:8A:DE:12:40:5A:78:0C:C2:C5:51:2C:89:30:BE:0F:D2:0D:C1:FB:3D:AF:26:5F:D5:D3:43:FB:1E:45:B9:D3:59:F1:7F:D9:10:D7:B3:5C:CF:C1:E7:9E:24:1C:2C:11:04:00:29:6C:21:6B:3A:D6:B5:86:70:B0:7B:BE:50:F9:22:61:9B:FC:A7:1A:3E:38:E3:54:FB:3F:D0:5F:8F:B4:2F:44:04:6F:C4:2D:DC:3B:96:5F:1D:0D:7B:51:A2:1B:EB:8E:AB:62:87:4E:A1:39:9A:EF:02:03:01:00:01*
Issuer Alternative Name	*ec_acc@catcert.net*
Subject Alternative Name	*ec-parlament@catcert.net*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*1E:13:98:EA:C2:42:59:55:B6:DE:2F:3E:CA:9F:C9:EA:CB:2E:2C:14*
Authority Key Identifier	*A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12* *CPS pointer: https://www.catcert.net/verCIC-2* *CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu https://www.catcert.net/verCIC-2]*
CRL Distribution Points	*http://epscd.catcert.net/crl/ec-acc.crl* *http://epscd2.catcert.net/crl/ec-acc.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*44:C5:0A:C8:0E:DB:E9:E5:52:E3:C9:6C:E5:BD:11:C8:37:C7:0F:56:A3:3A:CA:BC:F1:8D:8D:7A:9B:35:0E:07*

X509SubjectName

Subject CN:	*EC-PARLAMENT*
Subject OU:	*Parlament de Catalunya*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-03-15T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA PARLAMENT*
Name	*[en]*	*Qualified certificates issued by CA PARLAMENT*

Service digital identities

X509SubjectName

Subject CN:	*EC-PARLAMENT*
Subject OU:	*Parlament de Catalunya*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*HhOY6sJCWVW23i8+yp/J6ssuLBQ=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

5.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA PARLAMENT*
Name	*[en]*	*Qualified certificates issued by CA PARLAMENT*

Service digital identities

X509SubjectName

Subject CN:	*EC-PARLAMENT*
Subject OU:	*Parlament de Catalunya*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*HhOY6sJCWVW23i8+yp/J6ssuLBQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.5 - Service (withdrawn): Certificados Reconocidos emitidos por CA UR

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA UR*
Name	*[en]*	*Qualified certificates issued by CA UR*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *883402859421482711468908485941930327 6*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHkzCCBnugAwIBAgIQBqVtPLKBlSg/4Enn+TGdbDANBgkqhkiG9w0BAQUFADCB8zELMAkGA1UE
BhMCRVMxOzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2hvICBOSUYgUS0w
ODAxMTc2L1UkpMSgwIgYDVQQLExtYZXJ2ZWIzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2hvMTUwMwYD
VQQLExxWZWdldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UE
CxMsSmVyYXJxdWlhIEVudGl0YXRzIGRlIENlcnRpZmlyYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMT
BkVDLUFDQzAeFw0wMzEyMTcxMjE5N1FaFw0xOTEyMTYyMjI5N1FaMIIBGDELMAkGA1UEBhMCRVMx
OzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY2hvICBOSUYgUS0wODAxMTc2
LUkpMTQwMgYDVQQHEytQYXNzYXRnZSBkZSBsYSBDb25jZXBjaWlgMTEgMDgwMDggQmFyY2Vsb25h
MS4wLAYDVQQLEyVTZXJ2ZWIzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2hvIEVDV0yMTUwMwYDVQQL
EyxWZWdldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJDSUMtMzAoYykwMzEfMB0GA1UECxMW
VW5pdmVyc2l0YXRzIGkgLmVzZXJjYTE0MAwGA1UEAxMFRUMtVVVwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDNLfuny4EhhQwi8mQw1U6eG7WXtfZbxbYZK8SfKp+Fq4aTUH6sL3QdcfQe
fEeOuL2kOjEwfeDbXwH33Gu1WX5gdQQo7K4yzURmshDdk1u8at1iJe7YTMprF2k8kMzlApuDHT2P
lmdEK3pt7+DKv29Yc+Ko/FPxlRIXpKu8RFOgMXO9K142pwtn/1YNEK+IZrHmDAWxBJqwSb6QB395
sjenIVTw47Nqh8aJwrUJMHb20ip31CYgJ0HQdBsylghOwcMU+eGTifmfl21074Lc6i1oVKS/7B
zJ16fut3O2ICrZkaadz3DPtiHB36ZAQjDa819xDg1g5Ji414FpB1VmzJAgMBAAGjggL5MIIC9TAd
BgNVHRIEFjAUgRJIY19bY2NAY2F0Y2VydC5uZXQwHAYDVR0RBBUwE4ERZWNiZXJAY2F0Y2VydC5u
ZXQwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFEifjYbRy/HWiIf7
fxWiC1H4l/4LMIIBMQYDVR0jBIIBKDCCASSAFKDDl0SgN6VFyScAWtHxcKb6V2NoYHSpIH2MIHz
MQswCQYDVQQGEwJFUzE7MDkGA1UECMsyQWdlbmNpYSBDYXRhbGFuYSBkZSBDZXJ0aWZpY2FjaW8g
KE5IRiBRLTA4MDExNzYtSSkxKDAmBgNVBAsTH1NlcnZlaXMgUHVibGljcyBkZSBDZXJ0aWZpY2Fj
aW8xNTAzBgNVBAsTLFZlZ2V1IGh0dHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlcmFycmVsIChjKTAz
MTUwMwYDVQQLEyxKZXJhcnF1aWEgRW50aXRhdHMgZGUgQ2VydGlmaWNhY2hvIENhdGFsYW5lczEP
MA0GA1UEAxMGRUMtQUNDgbDuKcJr1CHeFKhirATz3cQBMIHcBgNVHSAEgdQwgdEwgc4GCysGAQQB
9XgBAwEMMIG+MCwGCCsGAQUFBwIBFiBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJDSUMtMjCB
jQYIKwYBBQUHAgIwgYAafkFxdWVzdCBjZXJ0aWZpY2F0IOlzIGV16HMg=m5pY2EgaSBleGNsdXNp
dmFtZW50IGEgRW50aXRhdHMgZGUgQ2VydGlmaWNhY2nzIGRlIENsYXNzZSAyLiBWZWdldSBodHRw
czovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJDSUMtMjBiBgNVHIR8EWzBZMFegVaBThidodHRwOi8vZXBz
Y2Qu Y2F0Y2VydC5uZXQvY3JsL2VjL WFjYy5jcmyGKGh0dHA6Ly9lcHNjZDIuY2F0Y2VydC5uZXQv
Y3JsL2VjL WFjYy5jcmwwDQYJKoZIhvcNAQEFBQADggEBACB5EXQhR4vaiDf6vIH51Ip5ZvQZtiU
b63J7Ph/tvYU2Ps7iIUuMLx9QPXx1cd2YqNHu/zPJ7TrfcEQzJryG7zujXWODuVXa98S/Lq/AKv
AU6Bro3vhnW1psWCISYPwnzmyv8tLFir0ftysgJIeo6FTWxrfjaD6esznnf6DZBRCjUWrwH3IXC9o
IOYGsF5IAGil9W9AmxSXJ9Jofhu+YRp8f9yridO4cc5QmksIAZ14sQ7u9IQSVHm1LEfm8EorvedU7
YhuldwMAeoZa9+/QMfOCp+HvU+JxF7/4F58IXBENbOis67BDyzE59rJsySaG4xFehxIp2g1fiSmD
YiioIl=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-ACC*

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu https://www.catcert.net/verarrel (c)03*

Issuer OU: *Serveis Publics de Certificacio*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-UR*

Subject OU: *Universitats i Recerca*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Valid from: *Wed Dec 17 13:19:51 CET 2003*

Valid to: *Mon Dec 16 23:59:59 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:2C:8B:A7:CB:81:21:85:0C:22:F2:64:30:D5:4E:9E:1B:B5:97:B5:F6:5B:C5:B6:19:2B:C4:9F:2A:9F:85:AB:86:93:5
0:7E:AC:2F:74:1D:79:F4:1E:7C:47:8E:B8:BD:A4:3A:31:30:7D:E0:DB:5F:01:F7:DC:6B:B5:59:7E:60:75:04:28:EC:AE:32:CD:44:66:B2:10:DD:93:5B:BC:6A:DD:62:25:EE:D8:4C:CA:6B:17:69:3C:90:CC:E5:02:9B:83:1D:3
D:8F:96:67:44:2B:7A:6D:EF:E0:CA:BF:6F:58:73:E2:A8:FC:53:F1:95:12:17:A4:AB:BC:44:53:A0:31:73:BD:2B:5E:36:A7:0B:67:FF:56:0D:10:AF:88:66:31:E6:0C:05:B1:04:9A:B0:4A:1E:90:07:7F:79:B2:37:A7:21:54:F0:E3:
B3:6A:87:C8:89:C2:B5:09:30:76:F6:D2:2A:77:D4:2D:20:27:41:D0:95:D0:6C:C8:88:21:D3:07:0C:53:E7:86:4E:27:E6:7F:69:76:D7:4E:F8:2D:CE:A2:D6:85:4A:4B:FE:C1:CC:9D:7A:7E:EB:77:3B:62:02:AD:99:1A:69:DC:F7:
0C:FB:62:1C:1D:FA:64:04:23:0D:AF:35:F7:10:E0:D6:0E:49:8B:8D:78:16:90:75:56:6C:C9:02:03:01:00:01

Issuer Alternative Name *ec_acc@catcert.net*

Subject Alternative Name *ec_ur@catcert.net*

Basic Constraints	*IsCA: true*
Subject Key Identifier	*48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B*
Authority Key Identifier	*A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12* *CPS pointer: https://www.catcert.net/verCIC-2* *CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu https://www.catcert.net/verCIC-2]*
CRL Distribution Points	*http://epscd.catcert.net/crl/ec-acc.crl* *http://epscd2.catcert.net/crl/ec-acc.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*87:00:D0:47:E5:07:11:16:F6:75:51:A4:39:39:98:D6:29:E6:6F:02:C7:B5:2E:61:8E:F4:F9:49:6E:73:47:56*

X509SubjectName

Subject CN:	*EC-UR*
Subject OU:	*Universitats i Recerca*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-03-15T01:00:00Z

Scheme Service Definition URI

URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*
URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

5.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.3*

5.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.5.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA UR*
Name	*[en]*	*Qualified certificates issued by CA UR*

Service digital identities

X509SubjectName

Subject CN:	*EC-UR*
Subject OU:	*Universitats i Recerca*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU:	*Serveis Publics de Certificacio ECV-2*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*SJ+NhtHL8daKUnt/FaIKUfiX/gs=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

5.5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.3*

5.5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.5.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por CA UR*

Name *[en]* *Qualified certificates issued by CA UR*

Service digital identities

X509SubjectName

Subject CN: *EC-UR*

Subject OU: *Universitats i Recerca*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *SJ+NhtHL8daKUnt/FaIKUfiX/gs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.3*

5.6 - Service (withdrawn): Certificados Reconocidos emitidos por CA URV

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por CA URV*

Name *[en]* *Qualified certificates issued by CA URV*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *132195878884101698654437343228416387356*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHuDCCBqCgAwIBAgIQY3QACu2RGYVJ6FAnJWZpHDANBgkqhkiG9w0BAQUFADCCARgxCzAJBgNV
BAYTAkVTMTswOQYDVQQKEzJBZ2VuYzIhIENhdGFsYW5hIGRlIENlcnRpZmljYWNpbyAoTkIGIFEt
MDgwMTE3Ni1JKTE0MDIGA1UEBxMrUGFzc2F0Z2UgZGUgbGEgQ29uY2VwY2lvIDExIDA4MDA4IEJh
cmNlbG9uYTEuMCwGA1UECxMIU2VydmVpcyBQdWJsaWNzIGRlIENlcnRpZmljYWNpbyBFQ1YtMjE1
MDMGA1UECxMsVmVnZXUgaHR0cHM6LyI5dXcuY2F0Y2VydC5uZXQvdmVyQ0lDLTIgKGMpMDMxHzAd
BgNVBAsTFlVuaXZlcnNpdGF0cyBpIFJlY2VyY2ExDjAMBgNVBAMTBUVDLVVSMB4XDTA5MDQxNzA5
NDcxOVoXDTE5MDQxNjIxNTk1OVowggEZMQswCQYDVQQGEwJFUzE7MDkGA1UEChMyQWdlbmNpYSBD
YXRhbGFuYSBkZSBDZXJ0aWZpY2FjaW8gKE5JRiBRLTA4MDExNzYtSSkxNDAyBgNVBAc TK1Bhc3Nh
dG9dIGRlIGxhIENvbmNlcGNpbyAxMSAwODAwOCBkYXIgZWxvbmEsKDAmBgNVBAsTH1NlcnZlaXMg
UHVibGljcyBkZSBDZXJ0aWZpY2FjaW8xNTAzBgNVBAsTLFZlZ2V1IGh0dHBzOi8vd3d3LmNhdGNl
cnQubmV0L3ZlckNJQy0zIChjKTA1MSUwIwYDVQQLExxVbml2ZXJzaXRhdCBSb3ZpcmEgaSBWaXJn
aWxpMQ8wDQYDVQQDEwZFQy1VUjYwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDm2r/
+kU/7tdv2XvSQr7zzjmrE9H1E7gAsN0OZgKc4fCvA1gtD8G3/Ta3sDRQ0jAnPrq/AJMHmqG1wiC
5hPUKNi7/H6u99NucmJl2UKhi71K8B0V1o30FoLwC/VmdkMWIl5pp5ob9Fu9yJk11M3uG6cMHdyF
MxUw7UARrCtmQCdrAH8WbrYKCL6lQt1rIOo6w66aWNhtgrx7H6g8U53LkUCp7J2q1pC+7RIo40IU
o+nA+sxKdocqbQj3N42B/Tx6Gy8xPebIABz9ZMBnADFtdqk8gufkmlFs+SlgsoScDWHiVE1fMcSG
PW2jDOUtm8q5j3yjJVlEhKbWRqqyLtXpAgMBAAGjggL3MIIC8zAcBgNVHREFTATgRFlY191ckBj
YXRjZXJ0Lm5ldDAdBgNVHREEFjAUgRlIYs1cnZAY2F0Y2VydC5uZXQwDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFLsuqS4w1JwQc7X9qXICPsNRl7k+MIIBMQYDVR0j
BIIBKDCCASSAFEifjYbRy/HWiU7fxWiCIH4l/4LoYH5pIH2MIHzMQswCQYDVQQGEwJFUzE7MDkG
A1UEChMyQWdlbmNpYSBDYXRhbGFuYSBkZSBDZXJ0aWZpY2FjaW8gKE5JRiBRLTA4MDExNzYtSSkx
KDAmBgNVBAsTH1NlcnZlaXMgUHVibGljcyBkZSBDZXJ0aWZpY2FjaW8xNTAzBgNVBAsTLFZlZ2V1
IGh0dHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlcmFycmVslChjKTAzM1UwMwYDVQQLEyxKZXJhcnF1
aWEgRW50aXRhdHMgZGUgQ2VydGlmaWNhY2lvIENhdGFsYW5lczEPMA0GA1UEAxMGRUMtQUNDghAG
pV88soGVKD/gSef5MZ1sMIHcBgNVHSAEgdQwgdEwgc4GCysGAQQB9XgBAwENMIG+MCwGCCsGAQUF
BwIBFiBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC9jcmwvZXJDSUMtMzCBjQYIKwYBBQUHAgIwgYAaRkFx
dWVzdCBjZXJ0aWZpY2F0IOIzIGVt6HMg+m5pY2EgaSBleGNsdXNpdmFtZW50IGEgRW50aXRhdHMg
ZGUgQ2VydGlmaWNhY2nzIGRlIG5pdmVsbCAzLiBWZWdldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5l
dC9ZXJDSUMtMzBgBgNVHR8EWTBXMFWgU6BRhiZodHRwOi8vZXBzY2QuY2F0Y2VydC5uZXQvY3Js
L2YjLXVyLmNvbHYmdHR0cDovL2Vwc2NkMy5jYXRjZXJ0Lm5ldC9jcmwvZWMtdXIuY3JsMA0GCSqG
SIb3DQEBBQUAA4IBAQCstmQJj+qYTb40FVOcrCgkza0ty/Ek2FrzJP8tEvxJa2ZY0quUFPcjiTSf
FY4h6imqiABFkHHTItOLCDfpilhCUpHDAieZAYCumj63dLixm70jXV9SGYBLdSKJod53SzovPWuj
7UBadCiksDTpK7zJU77RHUM3LZAWarHblr9cPAvibIlHiTh5e/SNkH5c/PcKon7bC4q+eHdlbrl+
g8YkIwPZZ7L903ZE0P50blM1/wFuy5JTsQESbGh1d8SuKX89uzDOXynTF5Ji57+Y5+EyhdsHR7
EladwcvInKb0oOY1AzZaEVTIWwMQHCMwyc8pC24mI3Chr+IuDopbiNo

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-UR*

Issuer OU: *Universitats i Recerca*

Issuer OU:	*Vegeu https://www.catcert.net/verCIC-2 (c)03*
Issuer OU:	*Serveis Publics de Certificacio ECV-2*
Issuer L:	*Passatge de la Concepcio 11 08008 Barcelona*
Issuer O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Issuer C:	*ES*
Subject CN:	*EC-URV*
Subject OU:	*Universitat Rovira i Virgili*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-3 (c)05*
Subject OU:	*Serveis Publics de Certificacio*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*
Valid from:	*Fri Apr 17 11:47:19 CEST 2009*
Valid to:	*Tue Apr 16 23:59:59 CEST 2019*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EB:9F:6A:FF:FA:42:3F:EF:A7:6F:D9:7C:92:42:2E:F3:CE:39:EB:13:D1:F5:11:38:00:B0:DD:0E:66:02:9C:E1:F0:AF:03:58:2D:0D:B1:B7:FC:2B:B7:B0:34:50:E2:30:27:3E:BA:BF:00:93:07:9A:A0:9D:D7:08:82:E6:13:D4:28:D9:7B:FC:7E:AE:F7:D3:6E:72:62:65:D9:42:A1:7F:BD:4A:F0:1D:15:D6:8D:F4:16:82:F0:0B:F5:66:76:43:16:94:8E:69:A7:9A:1B:F4:5B:BD:C8:99:25:D4:CD:EE:1B:A7:0C:1D:DC:85:33:15:30:ED:40:11:AC:2B:66:40:27:6B:00:7F:16:6E:B6:0A:08:BE:88:42:DD:6B:20:EA:3A:C3:AE:9A:58:D8:6D:82:BC:7B:1F:A8:3C:53:9D:CB:91:40:A9:EC:9D:AA:D6:90:BE:ED:12:28:E3:42:14:A3:E9:C0:FA:CC:4A:76:87:AA:6D:08:F7:37:8D:81:FF:BC:7A:1B:2F:31:3D:E6:DF:00:1C:FD:64:C0:67:00:31:6D:76:A9:3C:82:E7:E4:9A:51:6C:F9:29:60:B2:8E:5C:0D:61:E2:54:4D:5F:31:C4:86:3D:6D:A3:0C:E5:2D:9B:CA:B9:8F:7C:A3:25:57:C4:84:A6:D6:46:AA:B2:2E:D5:E9:02:03:01:00:01*
Issuer Alternative Name	*ec_ur@catcert.net*
Subject Alternative Name	*ec-urv@catcert.net*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*BB:2E:A9:2E:30:D4:9C:10:73:B5:FD:A9:77:C2:3E:C3:51:97:B9:3E*
Authority Key Identifier	*48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.15096.1.3.1.13* *CPS pointer: https://www.catcert.net/verCIC-3* *CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de nivell 3. Vegeu https://www.catcert.net/verCIC-3]*
CRL Distribution Points	*http://epscd.catcert.net/crl/ec-ur.crl* *http://epscd2.catcert.net/crl/ec-ur.crl*
Key Usage:	*keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A4:65:2E:D2:43:DA:CC:3F:EE:E1:F0:ED:7C:91:BD:B1:9A:9B:C2:25:E7:2A:5C:97:FD:A4:F1:F0:01:25:BA:A3*

Certificate fields details

Version: *3*

Serial Number: *132441740454361425377162905070003236530*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHuDCCBqCgAwIBAgIQY6NZ9DjTyilCd0YS4IsusjANBgkqhkiG9w0BAQUFADCCARgxCzAJBgNV
BAYTAkVTMTswOQYDVQQKDzJBZ2VuY2lhIENhdGFsYWSbIGRlIFNlcnRpZmljYWNpbyAoTkIGIFEt
MDgwMTE3Ni1JKTE0MDIGA1UEBxMrUGFzc2F0Z2UgZGUgbGEgQ29uY2VwY2lvIDExIDA4MDA4IEJh
cmNlbG9uYTEuMCwGA1UECxMlU2VydmVpcyBQdWJsaWNzIGRlIENlcnRpZmljYWNpbyBFQ1YtMjE1
MDMGA1UECxMsVmVnZXUgaHR0cHM6Ly93d3cuY2F0Y2VydC5uZXQvdmVyQ0lDLTIgKGMpMDMxHzAd
BgNVBAsTFlVuaXZlcnNpdGFlcyBpIFlY2VyY2ExDjAMBgNVBAMTBUVDLVVSMB4XDTA1MDUwMzA5
MzYxOFoXDTEzMDUwMzA5MzYxOFowggEZMQswCQYDVQQGEwJFUzE7MDkGA1UEChMyQWdlbmNpYSBD
YXRhbGFuYSBkZSBDZXJ0aWZpY2FjaW8gKE5JRiBRLTA4MDExNzYtSSkxNDAyBgNVBAcTK1Bhc3Nh
dGdlIGRlIGxhIENvbmNlcGNpbyAxMSAwODAwOCBCYXJjZWxvbmExKDAmBgNVBAsTH1NlcnZlaXMg
UHVibGIjcyBkZSBDZXJ0aWZpY2FjaW8xN1AzBgNVBAsTLFZlZ2VlIGh0dHBzOi8vd3d3LmNhdGNl
cnQubmV0L3ZlckNJQyQzIC hjKTA1MSU/wfwVDVQQLExxVbmlZXJzaXRhdCBSb3ZpcmFgaSBWaXJn
aWxpMQ8wDQYDVQQDEwZFQy1VUlYwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDm2r/
+kU/76dv2XySQi7zzjnrE9H1ETgAsN0OZgKc4fCvA1gtDbG3/Cu3sDRQ4jAnPrq/AJMHmqCd1wiC
5hPUKNl7/H6u99NucmJI2UKhi71K8B0V1o30FoLwC/VmdkMWll5pp5ob9Fu9yJk1IM3uG6cMHdyF
MxUw7UARrCtmQCdrAH8WbrYKCL60Qt1rIOo6w66aWNhtgrx7Hfg8U5ZLkUCp7IZq1pC+7Rlo40lU
o+nA+sxKdocqbQj3N42B/7x6Gy8xPebfABz9ZMBnADFtdqk8gufkmlFs+Slgso5cDWHiVE1fMcSG
PW2jDOUtm8q5j3yjJVIEhKbWRqqyLtXpAgMBAAGjggL3MIIC8zAcBgNVHRIEFTATgRFIY191ckBj
YXRjZXJ0Lm5ldDAdBgNVHREEFjAUgRJlYy11cnZAY2F0Y2VydC5uZXQwDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFLsuqS4w1lwQc7X9qXfCPsNRlT8+MIIBMQYDVR0j
BIIBKDCCASSAFEifjYbRy/HWiJ7kWiCIH4l/4LoYH5plH2MlHzMQswCQYDVQQGEwJFUzE7MDkG
A1UEChMyQWdlbmNpYSBDYXRhbGFuYSBkZSBDZXJ0aWZpY2FjaW8gKE5JRiBRLTA4MDExNzYtSSkx
KDAmBgNVBAsTH1NlcnZlaXMgUHVibGljcyBkZSBDZXJ0aWZpY2FjaW8xNTAzBgNVBAsTLFZlZ2V1
IGhldHBzOi8vd3d3LmNhdGNlcnQubmV0L3ZlcmFycmVsdCJyKTAzMTUwMwYDVQQLExxKZXJhcnF1
aWEgRW50aXRhdHMgZGUgQ2VydGlmaWNhY2lvIENhdGFsYW5lczEPMA0GA1UEAxMGRUMtQUNDghAG
pV88soGVKD/gSef5MZ1sMIHcBgNVHSAEgdQwgdEwgc4GCysGAQQB9XgBAwENMIG+MCwGCCsGAQUF
BwIBFiBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC9ZXJDSUMtMzCBjQYIKwYBBQUHAgIwgYAafkFx
dWVzdCBjZXJ0aWZpY2FlIlOtzIGVt6HMg+m5p3Y2EgaSBleGNsdXNpdmFlZW50IlGEgRW5taXthdHMg
ZGUgQ2VydGlmaWNhY2nzIGRlIG5pdmVsbCAzLiBWZWdlSBodHRwczovL3d3dy5jYXRjZXJ0Lm5l
dC92ZXJDSUMtMzBgBgNVHR8EWTBXMFWgU6BRhiZodHRwOi8vZXBzY2QuY2F0Y2VydC5uZXQvY3Js
L2VjLXVyLmNybHYnaHR0cDovL2Vwc2NkMi5jYXRjZXJ0Lm5ldC9jcmwvZWMtdXIuY3JsMA0GCSqG
SIb3DQEBBQUAA4IBAQCSeWvlaV2RJFD/ued6kqOjaIuJytcY8G3MMZ8C+csZ2Y1QVt0J1WIkXJgT
BBhbqAx012+K6Ny5HfZCzMUiD8+aR8TYBL4LfwJbgpg9229n0bWICE6+LKExXr5i2/ijcfcfcfKX
OqobzX8Jh5pKhELrjyiR4bEwL8mxhxUFfTnN3y1coKfQu96pJEXCC/p7DYMIHXcbJfoYeiTzKHg4
47SARVQAjuVfq0509b9BLGGtX5slkmIKVawyJ7KuenA6X8AQgCWQnwZz/u4LV4UzVW3KAluYvcSy
k1jpUsUgM4kFttwvXIeDzGX+JFjHdVvJ+l5RvrrSDxJp/71bsPTITJFM

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-UR*

Issuer OU: *Universitats i Recerca*

Issuer OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Issuer OU: *Serveis Publics de Certificacio ECV-2*

Issuer L: *Passatge de la Concepcio 11 08008 Barcelona*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-URV*

Subject OU: *Universitat Rovira i Virgili*

Subject OU: *Vegeu https://www.catcert.net/verCIC-3 (c)05*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Valid from: *Tue May 03 11:36:18 CEST 2005*

Valid to: *Fri May 03 11:36:18 CEST 2013*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EB:9F:6A:FF:FA:42:3F:EF:A7:6F:D9:7C:92:42:2E:F3:CE:39:EB:13:D1:F5:11:38:00:B0:DD:0E:66:02:9C:E1:F0:AF:03:58:2D:0D:B1:B7:FC:2B:B7:B0:34:50:E2:30:27:3E:BA:BF:00:93:07:9A:A0:9D:D7:08:82:E6:13:D4:28:D9:7B:FC:7E:AE:F7:D3:6E:72:62:65:D9:42:A1:7F:BD:4A:F0:1D:15:D6:8D:F4:16:82:F0:0B:F5:66:76:43:16:94:8E:69:A7:9A:1B:F4:5B:BD:C8:99:25:D4:CD:EE:1B:A7:0C:1D:DC:85:33:15:30:ED:40:11:AC:2B:66:40:27:6B:00:7F:16:6E:B6:0A:08:BE:88:42:DD:6B:20:EA:3A:C3:AE:9A:58:D8:6D:82:BC:7B:1F:A8:3C:53:9D:CB:91:40:A9:EC:9D:AA:D6:90:BE:ED:12:28:E3:42:14:A3:E9:C0:FA:CC:4A:76:87:AA:6D:08:F7:37:8D:81:FF:BC:7A:1B:2F:31:3D:E6:DF:00:1C:FD:64:C0:67:00:31:6D:76:A9:3C:82:E7:E4:9A:51:6C:F9:29:60:B2:8E:5C:0D:61:E2:54:4D:5F:31:C4:86:3D:6D:A3:0C:E5:2D:9B:CA:B9:8F:7C:A3:25:57:C4:84:A6:D6:46:AA:B2:2E:D5:E9:02:03:01:00:01

Issuer Alternative Name *ec_ur@catcert.net*

Subject Alternative Name *ec-urv@catcert.net*

Basic Constraints *IsCA: true*

Subject Key Identifier *BB:2E:A9:2E:30:D4:9C:10:73:B5:FD:A9:77:C2:3E:C3:51:97:B9:3E*

Authority Key Identifier *48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B*

Certificate Policies

Policy OID: 1.3.6.1.4.1.15096.1.3.1.13

CPS pointer: https://www.catcert.net/verCIC-3

CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de nivell 3. Vegeu https://www.catcert.net/verCIC-3]

CRL Distribution Points

http://epscd.catcert.net/crl/ec-ur.crl

http://epscd2.catcert.net/crl/ec-ur.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *88:33:D0:A9:1F:26:45:EF:EF:C3:B4:E0:0F:B8:97:C5:20:65:7E:BC:88:EA:F7:3B:9E:F0:F1:9A:2C:7B:A1:53*

X509SubjectName

Subject CN: *EC-URV*

Subject OU: *Universitat Rovira i Virgili*

Subject OU: *Vegeu https://www.catcert.net/verCIC-3 (c)05*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

ETSI 2016 - TSL HR - PDF/A-1b generator

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2018-03-15T01:00:00Z*

Scheme Service Definition URI

URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

5.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.6.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA URV*

Name [en] *Qualified certificates issued by CA URV*

Service digital identities

X509SubjectName

Subject CN: *EC-URV*

Subject OU: *Universitat Rovira i Virgili*

Subject OU: *Vegeu https://www.catcert.net/verCIC-3 (c)05*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *uy6pLjDUnBBztf2pd8I+w1GXuT4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.6.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

5.6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.6.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA URV*
Name	*[en]*	*Qualified certificates issued by CA URV*

Service digital identities

X509SubjectName

Subject CN:	*EC-URV*
Subject OU:	*Universitat Rovira i Virgili*
Subject OU:	*Vegeu https://www.catcert.net/verCIC-3 (c)05*
Subject OU:	*Serveis Publics de Certificacio*
Subject L:	*Passatge de la Concepcio 11 08008 Barcelona*
Subject O:	*Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C:	*ES*

X509SKI

X509 SK I	*uy6pLjDUnBBztf2pd8I+w1GXuT4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.6.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

5.7 - Service (granted): Qualified certificates issued by CA Ciutadania

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by CA Ciutadania*
Name	*[es]*	*Certificados Reconocidos emitidos por CA Ciutadania*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *154100517041182570311467181176543273551*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIF4TCCBMmgAwIBAgIQc+6uFePfrabUGpXs8lhiTzANBgkqhkiG9w0BAQsFADCB8zELMAkGA1UE
BhMCRVMxOzA5BgNVBAo1MkFnZWS5jaWEgQ2F0YWxhbmEgZGUgQ2VyZGlmaWNhY2hvIChOSUYgUS0w
ODAxMTc2LUkpMSgwJgYDVQQLEx9TZXJ2ZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2hvMTUwMwYD
VQQLEyxWZWdldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UE
CxMsSmVyYXJxdWltIEVudGl0YXRzIGRlIENlcnRpZmljYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMT
BkVDLUFDQzAeFw0xNDA5MTgwODIxMDBaFw0zMDA5MTgwODIxMDBaMIGCMQswCQYDVQQGEwJFUzEz
MDEGA1UECgwqQ09OUC9pNSQ0IGQURNSU5UIRSQUNJTyBPQk VSVEEgRE1gQ0FlQUcxYTllBMSowKAYD
VQQLDCFTZXJ2ZWlzIFDDumJsaWNzIGRlIENlcnRpZmljYWNpw7MxFjAUBgNVBAMMDUVDLUNpdXRh
ZGFuaWEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDFkHPRZPZIXTWZ5psJhbS/Gx+b
xcTpGrlVQHHtdkgGz77yTA7UZUFb2EQMncfbOhR0OkvQQn1aMvhOhFJSR6nI+cat2D+h/m/InMI1
MvHTS0AkYGZZsthnyC6KxqK2A/NApncrDreb70UlAQs4Sa0Ks41kR1W0zE+iFN+/P19P7AkLRl3b
XBCVd8w+DLhcwRrkf1FCDw6cEqaFm3cGgf5cbBDMaVYAweWTxwBZAq2RbQAWjE7mledcYghcZa4U
6bUmCBPuLOnO8KMFAvH+aRzaf3ws5/ZoOVmryyLLJVZ54peZOwnP9EL4OuWzmXCjBitXR2IAbIxs
5JYj57tIs45nAgMBAAGjggHaMIIB1jASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIB
BjAdBgNVHQ4EFgQUC2hZPotIoxUsdECCIl+HbLFNxUwHwYDVR0jBBgwFoAUoMOLRKo3pUW/l4Ba
0fF4opvpXY0wgdYGA1UdIASBzjCByzCByAYEVR0gADCBwzAxBggrBgEFBQcCARYlaHR0cHM6Ly93
d3cuYW9jLmNhdC9DQVRDZXJ0LlJlZ3VsYWNpbzCBtQYIKwYBBQUHAgIwtQx7QXF1ZXN0IGNlcnRp
ZmljYXQgw6lzIGVtw6hzIMO6bmlj YSBpIGV4Y2x1c2I2YW1lbnQgYSBFbnRpdGF0cyBkZSBDZXJ0
aWZpY2FjaC0zLiBWZWlddSBodHRwczovL3d3dy5hb2MuY2F0LI0NBVENlcnQvLmVsdWxh Y2lvMDMG
CCsGAQUFBwEBBCcwJTAjBggrBgEFBQcwAYYXaHR0cDovL29jc3Au Y2F0Y2VydC5jYXQw YgYDVR0f
BFswWTBXoFWgU4YnaHR0cDovL2Vwc2NkLmNhdGNlcnQubmV0L2NybC9lYy1hY2MuY3JshhodHRw
Oi8vZXBzY2QyLmNhdGNlcnQubmV0L2NybC9lYy1hY2MuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQCh
qFTjJAH5PydhLjLgEs68CyNNC1+vDuZXRhy22TI83JcvGmQrZosPvVILPsUXx+C06Piqmh48Q9S8
9X9K8w1SqDxPrzGcGEoRiKpnwvQzM4ArD9QxyCSjrxcx3Umg9Ai/sXQ+1IBf6xw4HIU/Ur1Wlp7pN
Hj0ZWLo106urqktcdcAFWme+/klis5fulabCSVPuT/QpwakPrtqOhRms8vgpKiXa/eLtL9ZiA28X
/Mker0zlAeTA7Z7uAnp6oPJTlZu1Gg1ZDJucTWWsLlO+P+Wzm3MRRlbcgdRzm4mdO7ubu26SzX/a
QXDhuih+eVxXDTCIS7GUxnjOp5j559X/N0A

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC-ACC*

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu https://www.catcert.net/verarrel (c)03*

Issuer OU: *Serveis Publics de Certificacio*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-Ciutadania*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Valid from: *Thu Sep 18 10:21:00 CEST 2014*

Valid to: *Wed Sep 18 10:21:00 CEST 2030*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:90:73:D1:64:F6:65:5D:35:99:E6:9B:09:85:B4:BF:1B:1F:9B:C5:C4:E9:1A:B9:55:40:71:ED:22:48:06:CF:BE:F2:4
C:0E:D4:65:41:5B:D8:44:0C:9D:C7:DB:3A:14:74:3A:4B:D0:42:7D:5A:32:F8:4E:6C:52:52:47:A9:C8:F9:C6:9F:D8:3F:A1:FE:6F:C8:9C:C9:75:33:21:F7:4B:40:24:60:66:59:B2:D8:67:C8:2E:8A:C6:A2:B6:03:F3:40:A6:77:2B
:3A:B7:A1:EF:45:0B:91:0B:38:E5:A3:8A:B2:2D:64:47:55:B4:CC:4F:A2:14:DF:BF:3F:5F:4F:EC:09:0B:46:5D:DB:5C:10:95:77:CC:3E:0C:B8:5C:C1:1A:E4:7F:51:42:0F:0E:9C:12:A6:85:9B:77:06:81:FE:5C:6C:10:CC:69:56:
00:C1:E5:93:C7:00:59:02:AD:91:6D:00:16:8C:4E:E6:95:E7:5C:62:08:5C:65:AE:14:E9:B5:26:08:13:EE:2C:E9:CE:F0:A3:05:02:F1:FE:69:1C:DA:7F:7C:2C:E7:F6:68:39:59:AB:CB:22:CB:25:56:79:E2:97:99:3B:09:CF:F4:42:
F8:3A:E5:B3:99:70:A3:06:27:D7:47:62:00:6E:5C:6C:E4:96:23:E7:BB:65:B3:8E:67:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *0B:68:59:3E:87:C8:A3:15:1A:E0:40:82:22:5F:9F:1D:B2:C5:37:15*

Authority Key Identifier *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.aoc.cat/CATCert/Regulacio

CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació. Vegeu https://www.aoc.cat/CATCert/Regulacio]

Authority Info Access *http://ocsp.catcert.cat*

CRL Distribution Points	*http://epscd.catcert.net/crl/ec-acc.crl* *http://epscd2.catcert.net/crl/ec-acc.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*0F:D9:9A:AE:1F:FC:D5:D9:F0:AD:76:ED:DD:CB:EF:6B:88:4C:C8:5C:16:BF:CF:A4:B5:24:61:55:D6:59:7E:D6*

X509SubjectName

Subject CN:	*EC-Ciutadania*
Subject OU:	*Serveis Públics de Certificació*
Subject O:	*CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.7.2 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA Ciutadania*
Name	*[es]*	*Certificados Reconocidos emitidos por CA Ciutadania*

Service digital identities

X509SubjectName

Subject CN:	*EC-Ciutadania*
Subject OU:	*Serveis Públics de Certificació*
Subject O:	*CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*
Subject C:	*ES*

X509SKI

X509 SK I	*C2hZPofIoxUa4ECCIl+fHbLFNxU=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2014-11-17T23:00:00Z*

5.8 - Service (granted): Qualified certificates issued by CA SectorPublic

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by CA SectorPublic*
Name	*[es]*	*Certificados Reconocidos emitidos por CA SectorPublic*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*151118660848720701053205649823964411794*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIF4zCCBMugAwIBAgIQcbBlOXyOB9JUGpZ/dVk3kjANBgkqhkiG9w0BAQsFADCB8zELMAkGA1UE
BhMCRVMxOzA5BgNVBAoTMkfzZW5jaWEgQ2F0YWxhbmEgZGUgQ2VyZGlmaWNhY2hvIChOSUYgUS0w
ODAxMTc2LUkpMSgwJgYDVQQLEx9TZXJZZWlzIFB1YmxpY3MgZGUgQ2VydGlmaWNhY2hvMTUwMwYD
VQQLEyxWZWdldSBodHRwczovL3d3dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UE
CxMsSmVyYXJxdWlhIEVudGl0YXRzIGRlIENlcnRpZmljYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMT
BkVDLUFDQzAeFw0xNDA5MTgwODIzMjdaFw0zMDA5MTgwODIzMjdaMIGlMQswCQYDVQQGEwJFUzEz
MDEGA1UECgwqQ09OU09SQ0lgQURCNSU5IU1RSQUNJTyBPQk VSVEEgRE1gQ0FLQUx VTlBMSowKAYD
VQQLDCFTZXJ2ZWlzIFDDumJsaWNzIGRlIENlcnRpZmljYWNpw7MxGDAWBgNVBAMMD0VDLVNlY3Rv
clB1YmxpYzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMuuTjExvPHbEIGJ3MU9RznS
cEIL86TETwZTO1GZsF1vRrGAJBV3QcXSXp9/r5b7cyq19DKLTuqRtKmnwSDfQCHbtv4mUWc8mbE
ZCRwQ2fjp1TRV1YGFnUZghUs32PjSrjkcZzTH5rAuS8uGXdTf4Anmns9wa+Ax705XFCd52sjiB4qU
Jtp6bMC7ECCHjWbLw0Akp4vPiPfbhLAxg400869eaMyEdkQsQYxgzyrEE9moNFRV66y3iB8env1Q
mN/NkMqdKlgy86HP22PrSed4f0NGSB2mz/Ti4qfGY1coroPnm5Q8IiWtvIDaBKi/DW5j+ogUJ7+2
w6fMAbVZUsHWo8MCAwEAAaOCAdowggHWMBIGA1UdEwEBwQIMAYBAf8CAQAwDgYDVR0PAQH/BAQD
AgEGMB0GA1UdDgQWBBRHPN4Ud7tq7fbeRqQL7Abhc9ez2TAfBgNVHSMEGDAWgBSgw4tEqzelR0+X
gFrR8Xiim+ldjTCB1gYDVR0gBIHOMIHLMIHlBgRVHSAAMIG/MDEGCCsGAQUFBwIBFiVodHRwczov
L3d3dy5hb2MuY2F0L0NBVENlcnQvUmVndWxhY2lvMIGJBggrBgEFBQcCAjB9DHtBcXVlc3QgY2Vy
dGlmaWNhdCDDqXMgZW3DqHMgw7puaWNhIGkgZXhjbHVzaXZhbWVudGlt0YXRzIGRlIENl
cnRpZmlYWNpw7MuIFZlZ2VlIGhldHBzOi8vd3d3LmFvYy5jYXQvQ0FUQ2VydC9SZWd1bGFjaW8w
MwYIKwYBBQUHAQEEJzAlMCMGCCsGAQUFBzABhhdoaHRwOi8vb2NzcC5jYXRjZXJ0LmNhdDBiBgNV
HR8EWzBZMFegVaBThododHRwOi8vZXBzY2QuY2F0Y2VydC5uZXQvY3JsL2VjLWFjYy5jcmwwDQYJKoZIhvcNAQELBQADggEB
dH A6Ly9lcHNjZDIuY2F0Y2VydC5uZXQvY3JsL2VjLWFjYy5jcmwwDQYJKoZIhvcNAQELBQADggEB
ADMROl0eqGiqUdlFFbagwKXb+K6rXGJAnfgY4bABMbblAZaDk1wXj23BO8JxLPMzgfiITXgswBS
ZTbTVEuyYQfP+lrUjP1ZGzXFPM+vKzsyF4K3s3FyfjdRmj0chumDFlao+gd9ttl6y7ySzHsgxZb1u/
i0L Sz4/48mY+pTxT1HCVw4zvzm9E9X26uKxn/UikI9B5EECHGChxw5Cx1RSF7THvhEBXfCQ6wsY6
32uvhi/H4QAkzmOZkh1PVzzehlsK2telJGfAt+xIxLHYvRUOTC5MRpSt2EzqvTjdsC8gKzGvgqYE
hZBqrq7VPnbUX9LuF9acflZXPsfNRalkAJW8smo=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *EC-ACC*

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu https://www.catcert.net/verarrel (c)03*

Issuer OU: *Serveis Publics de Certificacio*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Valid from: *Thu Sep 18 10:23:27 CEST 2014*

Valid to: *Wed Sep 18 10:23:27 CEST 2030*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:AE:4E:31:31:BC:F1:DB:11:F1:89:DC:C5:3D:47:39:D2:70:42:0B:F3:A4:C4:4F:06:53:3B:51:99:B0:5D:6F:46:B1:8
0:24:15:77:41:C5:D2:5E:9F:7F:AF:98:7B:73:2A:B5:F4:32:8B:4E:2A:91:B4:A9:A7:C1:20:DF:40:21:DB:B6:FE:26:20:95:9C:F2:66:C4:64:24:70:43:67:E9:D5:34:55:D5:81:85:9D:46:60:84:B8:77:D8:F8:D2:AE:39:5C:65:C4:C
7:E6:B0:1A:CB:86:5D:D2:13:7F:80:26:9A:CF:70:6B:E0:31:EF:4E:57:14:27:79:DA:C8:E2:07:8A:94:26:DA:7A:84:C0:BB:10:20:87:8D:66:CB:C3:40:24:A7:8B:CF:88:F7:DB:84:B0:31:83:8D:34:E3:AF:5E:68:CC:84:76:44
:2C:41:8C:60:CF:2A:C4:13:D9:A8:34:54:55:EB:AC:B7:88:1F:1E:9E:FD:50:98:DF:CD:90:CA:9D:2A:58:32:F3:A1:CF:DB:63:EB:49:E7:78:7C:E3:46:48:1D:A6:CF:F4:E2:E2:A7:C6:63:57:A8:AE:83:E7:9B:94:3C:22:25:AD:
BD:F0:DA:04:A8:BF:0D:6E:63:FA:88:14:27:BF:B6:C3:A7:CC:01:B5:59:52:C1:D6:A3:C3:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *47:3C:DE:14:77:BB:6A:4F:47:91:A9:02:FF:D4:06:E1:73:DC:E2:D9*

Authority Key Identifier *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.aoc.cat/CATCert/Regulacio

CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació. Vegeu https://www.aoc.cat/CATCert/Regulacio]

Authority Info Access *http://ocsp.catcert.cat*

CRL Distribution Points *http://epscd.catcert.net/crl/ec-acc.crl*

http://epscd2.catcert.net/crl/ec-acc.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *35:6A:5F:4D:99:4E:9E:FA:7C:AE:FC:49:17:68:91:1D:65:EC:25:97:74:65:B6:10:E2:F2:9A:A4:47:26:31:C3*

X509SubjectName

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2018-03-15T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

5.8.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

5.8.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.8.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

5.8.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

5.8.5 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA SectorPublic*
Name	*[es]*	*Certificados Reconocidos emitidos por CA SectorPublic*

Service digital identities

X509SubjectName

Subject CN:	*EC-SectorPublic*
Subject OU:	*Serveis Públics de Certificació*
Subject O:	*CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*
Subject C:	*ES*

X509SKI

X509 SK I	*RzzeFHe7ak9HkakC/9QG4XPc4tk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.8.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

5.8.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.8.6 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by CA SectorPublic*

Name *[es]* *Certificados Reconocidos emitidos por CA SectorPublic*

Service digital identities

X509SubjectName

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *RzzeFHe7ak9HkakC/9QG4XPc4tk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-11-17T23:00:00Z*

5.8.6.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

6 - TSP: ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC

.

TSP Name

Name	*[en]*	*ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC*
Name	*[es]*	*ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC*

TSP Trade Name

Name	*[en]*	*VATES-G63287510*
Name	*[en]*	*ANF AC*
Name	*[es]*	*ANF AC*
Name	*[en]*	*ANF Autoridad de Certificacion*

PostalAddress

Street Address	*[en]*	*Gran Vía de les Corts Catalanes, 996*
Locality	*[en]*	*Barcelona*
State Or Province	*[en]*	*Barcelona*
Postal Code	*[en]*	*8018*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Gran Vía de les Corts Catalanes, 996*
Locality	*[es]*	*Barcelona*
State Or Province	*[es]*	*Barcelona*
Postal Code	*[es]*	*8018*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.anf.es*
URI	*[en]*	*mailto:info@anf.es*

TSP Information URI

URI	*[en]*	*http://www.anf.es/en/*
URI	*[es]*	*http://www.anf.es*

6.1 - Service (withdrawn): Qualified certificate issued by ANF Server CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificate issued by ANF Server CA*
Name	*[es]*	*Certificado reconocido emitido por la CA ANF Server CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *41*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFyDCCBLCgAwIBAgIBKTANBgkqhkiG9w0BAQUFADCB2jELMAkGA1UEBhMCRVMxEjAQBgNVBAgT
CUlhcmNlbG9uYTFIMEYGA1UEBww/QmFyY2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IGh0
dHBzOi8vd3d3LmFuZi5lcy9hZGRyZXNzLyApMSowJQYDVQQKEx5BTkYgQXV0b3JpZGFkIGRlIEN1
cnRpZmlYWNpb24xFzAVBgNVBAsTDkFORiBDbGFzZSAxIENBMRMwEQYDVQQFEwpHLTYzMjg3NTEw
MRYwFAYDVQQDEw1BTkYgU2VydmVyIENBMB4XDTA1MDQwNTE0MjkwNVoXDTE1MDQwMzE0MjkwNVow
gdoxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlCYXJjZWxvbmExSDBGBgNVBAcMP0JhcmNlbG9uYSAo
c2VlIGN1cnJlbnQgYWRkcmVzcyBhdCBodHRwczovL3d3dy5hbmYuZXMvYWRkcmVzcy8gKTEnMCUG
A1UEChMeQUSGIEF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uMRcwFQYDVQQLEw5BTkYgQ2xhc2Ug
MSBDQTETMBEGA1UEBRMKRy02MzI4NzUxMDEWMBQGA1UEAxMNQU5GIFNlcnZlciBDQTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBALqSKcaiDlrLEhABwSTfPe4LX6lN+Jh1iH8kDtLaT5e
izfJW2872LbDiECQ9J0MXBBSsbP1X5EQ5v2ogBRf04u9XL0PI5IJN+Ny0maUC1x0lC9e8k7YA8az
zlaIHNl7/U8HTNS32I8pTXXyH1XPMdMcRgknHUXs8Yw0id57FqdDXoor6ZRDHtc+k21viT287rHI
t//IfcNfDW93ePLqLo3E15XMLFGWgtjcNR4s4azf/8nQqqfim5toZTK7IcCHNZUS/2biZamYzbm
jBaJiZfDUOj2QgGnd30QGZID6F1FyBXFhxsNkfLGOZx788AKmfjug29+QncRjsMfHHIvPRsCAwEA
AaOCAZUwggGRMB0GA1UdDgQWBBS+O/a0MbdzJEg5xVcTlHWqn4E/LDAMBgNVHRMEBTADAQH/MA4G
A1UdDwEB/wQEAwIBBjCB6gYDVR0gBIHiMIHfMIHcBgorBgEEAYGPHAEIMIHNMCwGCCsGAQUFBwIB
FiBodHRwczovL3d5dy5hbmYuZXMvQUMvZG9ydW1lbnRvczCBnAYIKwYBBQUHAgIwgYxagYxBbnR1
cyBkZSBhY2VwdGFyIGVzdGUgY2VydGlmaWNhZG8sIGNvbXBydWViZToKLUNvbmRpY2lvbmVzLCBs
aW1pdGFjaW9uZXMgeSB1c29zIGF1dG9yaXphZG9zIHNlZ3VuIENQIGEgbGEgcXVlIHNlIHNvbWV0
ZS4KLUVzdGFkbyBkZSB2aWdlbmNpYTAUBgorBgEEAYGPHBMBBAYbBDUtMzQwLgYKKwYBBAGBjxwq
BgQgGx5odHRwczovL3d5dy5hbmYuZXMvQUMvQUNUQVMvNDEwHwYDVR0jBBgwFoAUyv2DG3cyrI
OcVXE5R1qp+BPywwDQYJKoZIhvcNAQEFBQADggEBAHC1akrsji10BanorDUxdL dmQgkWxy7V1SOv
mpMX8I+4reU3JxEXFc4GaqjsJYfR4nZ2MSfnf1pjUHgG/Xw7f1AhrAju/wBN5agDTuHJV3Cpdon2
Z42LmDGCoI4N2ld2QeaFBtL5WQ5jETyTHBLmTKvzS3v6w2AXnt9wNubaoO44JjlpzCYEwUvz8qkA
LscchxypMYfDGW/bXHL8/Noo7Z76mw8askDAk0HCiCnzFGNsCRr+OvgcbbqSH2amUCBJuIqippHo
ehiEcsjH7g7ycl3hKsKmYyFMv34F1gOU16oSCwXjwYO0GmRdlhf+A+EODN9elmoJjtxqvQRmj1
wtI=

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA1withRSA*
Issuer CN:	*ANF Server CA*
Issuer SERIAL NUMBER:	*G-63287510*
Issuer OU:	*ANF Clase 1 CA*
Issuer O:	*ANF Autoridad de Certificacion*
Issuer L:	*Barcelona (see current address at https://www.anf.es/address/)*
Issuer ST:	*Barcelona*

Issuer C: *ES*

Subject CN: *ANF Server CA*

Subject SERIAL NUMBER: *G-63287510*

Subject OU: *ANF Clase 1 CA*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at https://www.anf.es/address/)*

Subject ST: *Barcelona*

Subject C: *ES*

Valid from: *Tue Apr 05 16:29:05 CEST 2005*

Valid to: *Fri Apr 03 16:29:05 CEST 2015*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BF:EA:48:A7:9A:88:39:6B:2C:48:40:07:04:93:7C:F7:B8:2D:7E:A5:37:E2:61:D6:21:FC:90:37:CB:69:3E:5E:8B:37:DF:5B:6F:3B:D8:B6:C3:88:40:90:F4:9D:0C:5C:10:52:B1:B3:E5:5F:91:10:E6:FD:A8:80:14:5F:D3:8B:BD:5C:BD:0F:23:92:09:37:E3:72:D2:66:94:0B:5C:74:94:2F:5E:F2:4E:D8:03:C6:B3:CE:56:A5:1C:D9:7B:FD:4F:07:4C:D4:B7:DA:5F:29:4D:75:F2:1F:55:CF:32:23:1C:46:09:27:1D:45:EC:F1:8C:34:89:DE:7B:16:A7:43:5E:8A:2B:E9:94:43:1E:D7:3E:93:6D:6F:89:3D:BC:EE:B1:C8:B7:FF:C9:7D:E3:5F:0D:6F:77:78:F5:2A:2E:8D:C4:8B:98:97:30:B1:46:5A:0B:63:70:D4:78:C7:86:B3:7F:FF:27:42:AA:9F:8A:6E:6D:A1:94:CA:EC:87:02:1C:D6:54:4B:FD:BC:89:9B:A6:63:38:66:8C:16:89:89:97:C3:50:E8:F6:42:01:A7:77:7D:10:19:92:03:E8:5D:45:C8:15:C5:87:1B:0D:91:F2:C6:39:9C:7B:F3:C0:0A:99:F8:EE:83:6F:7E:42:77:11:8E:C3:1F:1C:72:2F:3D:1B:02:03:01:00:01

Subject Key Identifier *BE:3B:F6:B4:31:B7:73:24:48:39:C5:57:13:94:75:AA:9F:81:3F:2C*

Basic Constraints *IsCA: true*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18332.1.8

CPS pointer: https://www.anf.es/AC/documentos

CPS text: [Antes de aceptar este certificado, compruebe:
-Condiciones, limitaciones y usos autorizados segun CP a la que se somete.
-Estado de vigencia]

Authority Key Identifier *BE:3B:F6:B4:31:B7:73:24:48:39:C5:57:13:94:75:AA:9F:81:3F:2C*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *71:D9:41:36:C6:0F:F5:74:6E:8D:93:23:27:A9:AE:D5:BE:6A:31:F4:2C:7F:55:B0:5A:37:4F:9B:6F:4D:27:27*

X509SubjectName

Subject CN: *ANF Server CA*

Subject SERIAL NUMBER: *G-63287510*

Subject OU: *ANF Clase 1 CA*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at https://www.anf.es/address/)*

Subject ST: *Barcelona*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

6.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4*

6.1.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.3.4*

6.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.1.4 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificate issued by ANF Server CA*
Name	*[es]*	*Certificado reconocido emitido por la CA ANF Server CA*

Service digital identities

X509SubjectName

Subject CN:	*ANF Server CA*
Subject SERIAL NUMBER:	*G-63287510*
Subject OU:	*ANF Clase 1 CA*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona (see current address at https://www.anf.es/address/)*
Subject ST:	*Barcelona*
Subject C:	*ES*

X509SKI

X509 SK I	*vjv2tDG3cyRIOcVXE5R1qp+BPyw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-05-11T00:00:00Z*

6.1.4.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4*

6.1.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.3.4*

6.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificate issued by ANF Server CA*

Name *[es]* *Certificado reconocido emitido por la CA ANF Server CA*

Service digital identities

X509SubjectName

Subject CN: *ANF Server CA*

Subject SERIAL NUMBER: *G-63287510*

Subject OU: *ANF Clase 1 CA*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at https://www.anf.es/address/)*

Subject ST: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *vjv2tDG3cyRIOcVXE5R1qp+BPyw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

6.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4*

6.1.5.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description

[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18332.3.4*

6.2 - Service (granted): Qualified certificate issued by ANF Assured ID CA1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificate issued by ANF Assured ID CA1*
Name	*[es]*	*Certificado reconocido emitido por la CA ANF Assured ID CA1*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *1374751084988*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIKyTCCCLGgAwIBAgIGAUAVjNG8MA0GCSqGSIb3DQEBBQUAMIIBCjELMAkGA1UEBhMCRVMxEjAQ
BgNVBAgMCUJhcmNlbG9uYTFYMFYGA1UEBwxPQmFvY2Vsb2ShlChzZWUgYXVycmVudCBhZGRyZXNz
IGF0IGhhdIAxLv9ZtXuYW5mLmVzL2VzL2FkZHIfc3MzZGJyZWNja W9uLmb0b WqgKTEnMCUGA1UE
CgwcQUSGIEF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uMRcwFQYDVQQLDA5BTkYgQ2xhc2UgMSBD
QTEaMBgGCSqGSIb3DQEJARYLaW5mb0BhbmYuZXMxEjAQBgNVBAUTCUc2MzI4NzU3xMDEbMBkGA1UE
AwwSQUSGIEdsb2JhbCBSb290IENBMB4XDTEzMDcyNTExMTgwNFoXDTIzMDcyMzExMTgwNFowggEh
MQswCQYDVQQGEwJFUzESMBAGA1UECAwIQmFyY2Vsb25hMVgwVgYDVQQHDE9CYXJjZWxvbmFgKHNl
ZSBjdXJyZW50IGFkZHIlc3MgYXQgaHR0cDovL3d3dy5hbmYuZXMvZXMvYWRkcmVzcy1kaXJlY2Np
b24uaHRtbCApMScwJQYDVQQKDB5BTkYgQXV0b3JpZGFkIGRlIENlcnRpZmlyYWNpb24xLjAsBgNV
BAsMJUFORiBBdXRvcmlkYWQgSW50ZXJlZWRpYSBkZSBJZGVudGlkYWQxGjAYBgkqhkiG9w0BCQEW
C2luZm9AYW5mLmVzMRIwEAYDVQQFEwlHNjMyODc1MTAxGzAZBgNVBAMMEkFORiBBc3N1cmVkIEIE
IENBMTCCAidwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJx79lIt/H2YDOok+e6MtcTgp+yB
V/oKIUt/fXHREniydpaNBRB4mUAC1olFJbGXCFAVg+ZEfrXziY172aRXVH3MMeV4BRFZkNc1+s
FqRyoMbCSTe8t7f93vlli/CMWJSYjhBG1xjn/3vFrZWLYFUOsu5z5ZeG8PoltsM33cwqOI8URhoI
i0Bdkg1/AnLBHIb/U/rmmK8aV1nwgrTuGO5W2SvRR1QARNwxuLnitMtOt1erWUc1tKAaBqIYIZM9
4mz9cW8jxtukBJCam+vnLnwDFJKr4HfGjMcQlRc72zsD5/k4Mmt4kom7VLro44ZxMJCBMAkgUYt
PF760gcHxIfQDf9XN2Q+JRJlhvZSMMvdBOg9VmamDog4Sg19zaDfWDoy3GBObHCOS9pCF0pQ/2
9vRk2woYeI3gKhmsHiY66BhD8SKTm7UJ90bQhfIwV4NZqfbeU/wub71J166beJOy8Hbrwlpyjs P6
ut1UMIDQ4xcUB+v9S6hiOWOrRPaemyqjWamrtgds4p+anPHyWRBhH4R43RG6+TUqPnYkXE2iFm
n0YsdY4KhAnT9V1a9lcIsaD3ORonMVSTPEiIOfy87UPe1cgAleauu3+c9psGifEdhxu1a6JsBIBlM
OPab9Yub4fra7pLE0v1SkCelsLUdv+0cqNcJ8ys6GJKNvOWLTAgMBAAGjggQYMIIEFDAdBgNVHQ4E
FgQUNS4t5ikcv4vZSnycK+CVR9HGTz0wHwYDVR0jBBgwFoAUh/qcs1J2dcxJSiBvW3CWj53vuxcw
DwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwggEhBgNVHSAEggEYMIIBFDCCARAGBFUd
IAAwggEGMIHYBggrBgEFBQcCAjCBxxqByEFORiBBQyBlbWlzb3IgZGUgY2VydGlmaWNhZG9zIHJl
Y29uZ2NpZG9zIGNvbmZvcm1lIGxhIExlcSA1OS8yMDAzIEVzcGHxYS4gQ3VbbHF1aWVyIHVzbyBk
ZSBlc3RlIGNlcnRpZmlyYWRvIGltcGxpY2EgbGEgYWNlcHRhY2lvbiBkZSBsYSBDUFMgcSBkZSBs
YXMgbGltaXRhY2lvbmVzIGRlIHUlc3BvbnNhYmlsaWRhZCBlbiBlbCBlc3RhYmxlY2lkYXMuMCkG
CCsGAQUFBwIBFh1odHRwczovL3d3dy5hbmYuZXMvZG9jdW1lbnRvczCCATYGA1UdIwSCAS0wggEp
MDegNaAzhjFodHRwczovL3d3dy5hbmYuZXMvY3JsL0FORl9HbG9lYWxfUm9vdF9DQV9hcmwuY3Js
MDegNaAzhjFodHRwczovL2Nyb5hbmYuZXMvY3JsL0FORl9HbG9lYWxfUm9vdF9DQV9hcmwuY3Js
MIG0oIGxoIGuhlFsZGFwOi8vbGRhcC5hbmYuZXM6Mzg5L2NuPUFORl9HbG9lYWxfUm9vdF9DQV9h
cmwuY3JsL29lPUFORl9HbG9lYWxfUm9vdF9DQSxkYz1hbmakWTBXMRMwEQYKCZImiZPyLGQBGRYD
YW5mMSMwIQYDVQQDDBpBTlZfR2xvYmFsX1Ivb3RfQ0FfYXJsLmNybDEbMBkGA1UECwwSQUSGX0ds
b2lhbF9Sb290X0NBMDgGCCsGAQUFBwEBBCwwKjAoBggrBgEFBQcwAYYcaHR0cHM6Ly9vYJNwLmFu
Zi5lcy9zcGFpbi9BVjCCARYGA1UdEQSCAQ0wggEJghJodHRwczovL3d3dy5hbmYuZXOBC2luZm9A
YW5mLmVzpHIMdIHiMTQwMgYDVQQJDCtHcmFuIFZpYSBkZSBsZXMgQ29ydHMgQ2F0YWxhbmVzLiA5
OTYuIDAMDE4MRIwEAYDVQQHDAlCYXJjZWxvbmEsIAIBgNVBAoMHkFORiBlbiXRvcmlkYWQgZGUg
Q2VydGlmaWNhY2lvbjESMBAGA1UEBRMJRzYzMjg3NTEwMVkwVwYDVQQLDFBJbnNjcml0YSBlbiBl
bCBNaW5pc3RlcmlvIGRlbCBJbnRlcmlvciBkZSBFc3Bhw7FhIGNvbiBlbCBudW1lcm8gbmFjaW9u
YWwgMTcxLjQ0MzANBgkqhkiG9w0BAQUFAAOCAgEAxzqDM0IEfwRNHJ6uwuHJcPQk1AtZ4/twjkJ
uAc7DNSe9vfmI312wumAmYOwJiVQWVoTYstgFc1jb6VqM9URp20kiXUP+jQWukKoaKIFIT4i+Lv7R
vCPH4wnyrOgVdZTEBJ488t2IQRPwAh6b41Ha1Gfk2f6oDEgb+YdxRBWkRGw5u5Dw/QjFOt7X9QDW
xC3k/QRaZ2WhQQFm2npxLeXhO+KAF2sI+nEU/ognUn609CgmVHQU4OnEEd2YB7PNiH3bXWPPsMxtJ
h7s8qWeQJRbnXoy3mcIfoCnv0ukYkiToRSOtMaeitMxc2e/9VINcIXbaA+sS62Tg1ZU5YQAFFrD
8xXOCuiMGBWkQbLZAwxoFWZk2rt+hvL91Ff06wFxLtMXpLR4TDJvKYH/459Kwv9/0YGX3y9JSrgPPT
JpTFY5ecBggKbFl/ht/hWkgrvVWN0LF0tY9t8Ktfi63rdy4xiz4Lnplo0ROJ++9TWJUmSzRTibpUX
vADYASX1d4383Vs40tPntKqeN9o4aMPosHLhPucbHDgDfpEW3TaHpzuTfHo4/hUMiEbefQZXz7Z7
+ap4SEHE92f9f8VfjWYBj8iA5I57x5geefBW3g+xOYiIE7GEpFuLsWwgNfyFIlzAePOyhDzILGv8R
FlFOtfvIlZ7H0j24r0HWxOXSGkdmIupdEnb04iI=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ANF Global Root CA*

Issuer SERIAL NUMBER: *G63287510*

Issuer E: *info@anf.es*

Issuer OU: *ANF Clase 1 CA*

Issuer O: *ANF Autoridad de Certificacion*

Issuer L: *Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*

Issuer ST: *Barcelona*

Issuer C: *ES*

Subject CN:	*ANF Assured ID CA1*
Subject SERIAL NUMBER:	*G63287510*
Subject E:	*info@anf.es*
Subject OU:	*ANF Autoridad Intermedia de Identidad*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*
Subject ST:	*Barcelona*
Subject C:	*ES*
Valid from:	*Thu Jul 25 13:18:04 CEST 2013*
Valid to:	*Sun Jul 23 13:18:04 CEST 2023*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:7B:F4:89:6D:FC:7D:98:0C:EA:24:F9:EE:8C:AD:C4:E0:A7:EC:81:57:FA:0A:95:4B:7F:7C:85:C7:44:49:E2:C9:DA:5A:34:14:41:E2:B9:94:00:2D:68:20:52:5B:19:70:85:01:58:3E:64:47:EB:5F:3B:58:97:BD:9A:45:75:47:DC:C3:1E:57:80:51:15:99:0D:7B:5F:AC:16:A4:72:A0:C6:C2:E5:37:BC:B7:B7:FD:DE:F9:65:8B:F0:8C:58:94:98:8E:10:46:D7:18:E7:FF:7B:C5:AD:95:8B:60:55:0E:B2:EE:73:E5:97:86:F0:FA:25:B6:C3:37:DD:CC:2A:38:8F:14:46:1A:08:8B:40:5D:92:0D:7F:02:72:C1:1D:F6:FF:53:FA:E7:98:AF:1A:57:5B:70:82:B4:EE:18:EE:56:D9:2B:D1:47:54:00:44:DC:31:B8:B9:E2:B4:CB:4E:B7:57:9F:59:47:35:B4:A0:1A:06:A2:18:7D:93:3D:E2:6C:FD:79:6F:23:C6:2B:A4:04:90:9A:9B:EB:E7:2E:2C:03:14:99:2B:E0:7B:4A:8C:C7:10:95:17:3B:DB:3B:03:E7:FF:E4:E0:C9:BA:E2:4A:26:ED:52:EB:A3:8E:19:C4:C2:42:04:C0:24:81:46:2D:3C:5E:FA:D2:07:07:C4:87:D0:0D:F7:ED:5C:DD:90:F8:94:49:96:1B:D9:48:C3:2F:74:13:A0:F5:59:9A:98:3A:20:E1:28:35:F7:36:83:7D:60:E8:CB:71:81:39:B1:C2:39:28:BD:A4:21:74:A5:0F:F6:F6:F4:64:DB:0A:18:7A:5D:E0:2A:19:AC:1E:26:3A:E8:18:43:F3:92:93:9B:B5:09:F7:46:D0:85:F2:22:C1:5E:0D:66:A7:DB:79:4C:2E:6F:BD:49:D7:AE:9B:78:93:B2:F0:76:EB:C2:5A:72:8E:C3:FA:BA:DD:54:30:80:D0:E3:17:14:07:EB:FD:4B:A8:62:39:63:AB:44:F6:9E:9B:2A:A3:59:A9:AB:D2:07:6C:E2:9F:9A:9C:FB:48:C9:64:41:84:7E:11:E3:74:46:EB:E4:D4:8E:A3:E7:62:45:C4:DA:21:66:9F:46:2C:E1:8E:0A:84:09:D3:F5:5D:5A:F6:57:88:B1:A0:F7:39:1A:27:35:54:93:3C:48:B5:38:8C:BC:ED:43:DE:D5:E8:C0:95:E6:B0:BB:7F:9C:F6:9B:2D:1A:D1:1D:87:1B:B5:6B:A2:6C:04:19:4C:38:F6:9B:62:E6:F8:7E:B6:BB:A4:B1:34:BF:54:A4:09:E2:2C:2D:47:6F:FB:47:2A:36:B2:7C:CA:CE:86:24:A3:6F:39:62:D3:02:03:01:00:01*
Subject Key Identifier	*35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*
Authority Key Identifier	*87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17*
Basic Constraints	*IsCA: true*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS text: [ANF AC emisor de certificados reconocidos conforme la Ley 59/2003 España. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]* *CPS pointer: https://www.anf.es/documentos*
CRL Distribution Points	*https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl* *https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl* *ldap://ldap.anf.es:389/cn=ANF_Global_Root_CA_arl.crl,ou=ANF_Global_Root_CA,dc=anf* *DC=anf,CN=ANF_Global_Root_CA_arl.crl,OU=ANF_Global_Root_CA*
Authority Info Access	*https://ocsp.anf.es/spain/AV*
Subject Alternative Name	*https://www.anf.es* *info@anf.es* *OU=Inscrita en el Ministerio del Interior de España con el numero nacional 171.443, SERIALNUMBER=G63287510, O=ANF Autoridad de Certificacion, L=Barcelona, STREET=Gran Via de les Corts Catalanes. 996. 08018*
Key Usage:	*keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *95:76:87:4B:7C:0B:40:8C:2F:C6:2E:B5:74:96:F1:BA:8F:22:04:63:C5:8D:29:02:A2:65:36:18:71:4B:CF:4F*

Certificate fields details

Version: *3*

Serial Number: *450373866247584128*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIKzjCCCLagAwIBAgIIBkAMpSnOeYAwDQYJKoZIhvcNAQELBQAwggEKMQswCQYDVQQGEwJFUzES
MBAGA1UECAwJQmFyYZVsb25hMVgwVzYDVQQHDE9CYXJjZWxvbmEgKHN0ZSBqXJvZW50IGFkZHJl
c3MgYXQgaHR0cDovL3d3dy5hbmYuZXMvYWRkcmVzcy1kaXJlY2Npb24uaHRtbCApMScwJQYD
VQQKDB5BTkYgQXV0b3JpZGFkIGRlIENlcnRpZmlqYWNpb24xFzAVBgNVBAsMDkFORiBDbGFzZSAx
IENBMRowGAYJKoZIhvcNAQkBFgtpbmZvQGFuZi5lczESMBAGA1UEBRMJRzY2Mjg3NTEwMRswGQYD
VQQDDBJBTkYgR2xvYmFsIFJvb3QgQ0EwIBhcNMTQwMzAzMTExNzIzWhcNMjQwMjI5MTExNzIzWjCC
ASExC2AJBgNVBAYTAkVTMRIwEAYDVQQIDAlCYXJjZWxvbmExWDBWBgNVBAcMT0JhcmNlbG9uYSAo
c2VlIGN1cnJlbnQgYWRkcmVzcyBhdCBodHRwOi8vd3d3LmFuZi5lcy9lcy9hZGRyZXNzLWRpcmVj
Y2lvbi5odG1sICksJzAlBgNVBAoMHkFORiBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhYV2lvbjEuMCwG
A1UECwwIQUS5GIEF1dG9yaWRhZCBJbnRlcm1lZGlhIGRlIEk2W50aWRhZDEaMBgGCSqGSib3DQEJ
ARYLaW5mb0BhbmYuZXMxEjAQBgNVBAUTCUc2MzHNzUxMDEhMBkGA1UEAwwSQU5GIEFzc3VyZWQg
SUQgQ0ExMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAnHv0iW38fZgM6tT57oytxOCn
7IFX+gqVS398hcdESeLJ2lo0FEHiuZQALWggUlsZciUBWD5kR+ttO1xVzpFdUfcwx5XgFEVmQ17
X6wWpHKgxsLlN7y3t/3e+WWL8IxYIJoEEbXGOEo8WtlYtgVQ6v7nPIl4dw+iW2wzfdzCo4jxRG
GgtLQE2SDX8CssEd9v9T+ueYrxpXW3CCtOMY7lbZK9FHVABE2DG4uck0t063V59ZRzW0uBoGohh9
kz3ibP15bvPGK6QEkJqb6+cuLAMUmSvge0qMxxCVFzvbOwPn/+TgybtSibtUuijhnEwkIEwCSB
Ri08XvrSBwtEh9AN9/1c3ZD4lEmWG9llwy90E6D1WZqYOiDhKDX3NoN9YOjLeYE5scI5KL2kIXSl
D/b29GTbCbh6XcAqGawcJroGEPzkpObtQn3RtCF8iLBXg1mp9I5TC5vvUnXrpl4k7LwduvCWnKO
w/q63VQwgNDjFxQH6/1LgGI5Y6tE9p6bKqNZqavSB2znx5qc+0jIZTGEIhHjdEbr5NSOo+diRcT1a
IWafRtzhjgqECdP1XVr2V4ixoPc5Gic1VJM8SLU4jLztQ97V6MCV5rC7f5z2my0a0R2HG7VromwE
GUw49pti5vh+truksTS/VKQJ4iwtR2/7Ryo2snzKzoYko285YtMCAwEAAaOCBBswggQXMB0GA1Ud
DgQWBBQ1Li3mKRy/i9lKOJ4u4JVH0cZPPTABgNVHSMEGDAWgBSH+p7fUnZI7EIKIG9bcfaPne+7
FzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjCCASQGA1UdIASCARswggEXMIIBEwYE
VR0gADCCAQkwgdgGCCsGAQUFBwICMIHLGoHIQU5GIEFDIGVtaXNvciBkZSBjZXJlaWZpY2Fkb3Mg
cmVjb25vY2lkb3MgY29uZm9ybWUgbGEgTGV5IDU5LzIwMDMgRXNwYIFhLiBDdWFscXVpZXIgdXNv
IGRlIGVzdGUgY2VydGlmaWNhZG8gaW1wbGlyYSBsYSBhY2VwdGFjaW9uIGRlIGxhIENQUyB5IGRl
IGxhcyBsaW1pdGFjaWYuZXMgZGUgcmVzcC9ucI2iaWxpZGFkIGVuIGVsIGVzdGFibGVjaWRhcy4w
LAYIKwYBBQUHAgEWIGh0dHBzOi8vd3d3LmFuZi5lcy9lcy9kb2N1bWVudG9zMIIBNgYDVR0fBIIB
LTCCASkwN6A1oDOGMWh0dHBzOi8vd3d3LmFuZi5lcy9jcmwvQU5GX0dsb2Jhbf9Sb290X0NBX2Fy
bC5jcmwwN6A1oDOGMWh0dHBzOi8vY3JsLmFuZi5lcy9jcmwvQU5GX0dsb2JhbF9Sb290X0NBX2Fy
bC5jcmwwgbSggbGigaG6UWxkYXA6Ly9sZGFwLmFuZi5lczozODkvY24${9QU5GX0dsb2Jhbf9Sb290
X0NBX2FybC5jcmwsb3U${9QU5GX0dsb2Jhbf9Sb290X0NBLGRjPWFuZqRZMfcxEzARBgoJkiaJk/Is
ZAEZFgNhbmYxIzAhBgNVBAMMGkFORl9HbG9YWxfUm9vdF9DQV9hcmwuY3JsMRswGQYDVQQLDBJB
TkZfR2xvYmFsX1Jvb3RfQ0EwNwYIKwYBBQUHAQEEKzApMCcGCCsGAQUFBzABhhtodHRwOi8vb2Nz
cC5hbmYuZXMvc3Bha4vQVYwgsEXBgNVHREEgsEOMIIBCoIRaHR0cDovL3d3dy5hbmYuZXOBC2Iu
Zm9AYWSmLmVzpIHnMIIfkMTQwMgYDVQQDCCHcmFuIFZpYSBkZSBsZXMgQ29vdHMgQ2F0YWxhbmVz
LiA5OTYuIDA4MDE4MRIwEAYDVQQHDAlCYXJjZWxvbmExJzAlBgNVBAoMHkFORiBBdXRvcmlkYWQg
ZGUgQ2VydGlmaWNhY2lvbjETMBEGA1UEBRMKIEc2MzI4NzUxMDFaMFgGA1UECwxRIEluc2NyaXRh
IGVuIGVsIE1pbmlzdGVyaW8gZGVsIEludGVyaW9yIGRlIEVzcGHDsWEgY29uIGVsIG51bWVybyBu
YWNpb25hbCAxNzIuNDQzMA0GCSqGSIb3DQEBCwUAA4ICAQAjD1enkC+qtEpWcgcWwxCeMRzJ48
Y9EA5iKFgW2qC4Y00mIW8xoZODhjRrs4FtEu3OfyNVr1ivuuJDzaQp8io/HmGcapUFZ3ddlHQIY
VNZBJL1PpO+pgv4JJmFCRsQX0QMa4I7TwA/F1jCUbVIqJshGoktq2x9VORs T8w7qdEoN+ulti6oW
JLmAWzwiVPl2btNI0E=JkVqueuVyCYCdEDrq2h+nyJhBcfNPnF7wcMYhjdJOcTIln5QuBYrSuXC
ZnbQrGuKYH5C5Ih6hjdcbrM0PECodYT683jrXo0Y1aoIZ+5iCNqVg8edxEHtQyLdcRzJxbgKcS/F
740+t1NsCtoXPzz/VKT3AbbaXrAkYIkbsZNZpZ89ah+vyWPDObnNggFOE1wP41R6iEGrYMI3xcj
dDTdNEkJ4y1dDJnDzNZRctvHEjTppAFN4kozHW7MNk7jAkk3Rz87dlQ0eYdvj/ECx7kPNZixv2E
ZnZtI39B+9BUzFi8/AhaZw0RVSqFEMyZMCwldx/xNvJ78b2nOTGpnzh/OcDFvKs2e7yTVzgAup
4cPScqG4foCBfebNvSnXtOmuTptvgeSoQp+8gk7kDWkysUL2OUGr23z/TQzw/i1giFvipaKGFel
6A1t7WNF4B2askrDnWukHN13KoUlZ0kU9TNg0+6KijN98g==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF Global Root CA*

Issuer SERIAL NUMBER: *G63287510*

Issuer E: *info@anf.es*

Issuer OU: *ANF Clase 1 CA*

Issuer O: *ANF Autoridad de Certificacion*

Issuer L: *Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*

Issuer ST: *Barcelona*

Issuer C: *ES*

Subject CN: *ANF Assured ID CA1*

Subject SERIAL NUMBER: *G63287510*

Subject E: *info@anf.es*

Subject OU:	*ANF Autoridad Intermedia de Identidad*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*
Subject ST:	*Barcelona*
Subject C:	*ES*
Valid from:	*Mon Mar 03 12:17:23 CET 2014*
Valid to:	*Thu Feb 29 12:17:23 CET 2024*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:7B:F4:89:6D:FC:7D:98:0C:EA:24:F9:EE:8C:AD:C4:E0:A7:EC:81:57:FA:0A:95:4B:7F:7C:85:C7:44:49:E2:C9:DA:5A:34:14:41:E2:B9:94:00:2D:68:20:52:5B:19:70:85:01:58:3E:64:47:EB:5F:3B:58:97:BD:9A:45:75:47:DC:C3:1E:57:80:51:15:99:0D:7B:5F:AC:16:A4:72:A0:C6:C2:E5:37:BC:B7:B7:FD:DE:F9:65:8B:F0:8C:58:94:98:8E:10:46:D7:18:E7:FF:7B:C5:AD:95:8B:60:55:0E:B2:EE:73:E5:97:86:F0:FA:25:B6:C3:37:DD:CC:2A:38:8F:14:46:1A:08:8B:40:5D:92:0D:7F:02:72:C1:1D:F6:FF:53:FA:E7:98:AF:1A:57:5B:70:82:B4:EE:18:EE:56:D9:2B:D1:47:54:00:44:DC:31:B8:B9:E2:B4:CB:4E:B7:57:9F:59:47:35:B4:A0:1A:06:A2:18:7D:93:3D:E2:6C:FD:79:6F:23:C6:2B:A4:04:90:9A:9B:EB:E7:2E:2C:03:14:99:2B:E0:7B:4A:8C:C7:10:95:17:3B:DB:3B:03:E7:FF:E4:E0:C9:BA:E2:4A:26:ED:52:EB:A3:8E:19:C4:C2:42:04:C0:24:81:46:2D:3C:5E:FA:D2:07:07:C4:87:D0:0D:F7:FD:5C:DD:90:F8:94:49:96:1B:D9:48:C3:2F:74:13:A0:F5:59:9A:98:3A:20:E1:28:35:F7:36:83:7D:60:E8:CB:71:81:39:B1:C2:39:28:BD:A4:21:74:A5:0F:F6:F6:F4:64:DB:0A:18:7A:5D:E0:2A:19:AC:1E:26:3A:E8:18:43:F3:92:93:9B:B5:09:F7:46:D0:85:F2:22:C1:5E:0D:66:A7:DB:79:4C:2E:6F:BD:49:D7:AE:9B:78:93:B2:F0:76:EB:C2:5A:72:8E:C3:FA:BA:DD:54:30:80:D0:E3:17:14:07:EB:FD:4B:A8:62:39:63:AB:44:F6:9E:9B:2A:A3:59:A9:AB:D2:07:6C:E2:9F:9A:9C:FB:48:C9:64:41:84:7E:11:E3:74:46:EB:E4:D4:8E:A3:E7:62:45:C4:DA:21:66:9F:46:2C:E1:8E:0A:84:09:D3:F5:5D:5A:F6:57:88:B1:A0:F7:39:1A:27:35:54:93:3C:48:B5:38:8C:BC:ED:43:DE:D5:E8:C0:95:E6:B0:BB:7F:9C:F6:9B:2D:1A:D1:1D:87:1B:B5:6B:A2:6C:04:19:4C:38:F6:9B:62:E6:F8:7E:B6:BB:A4:B1:34:BF:54:A4:09:E2:2C:2D:47:6F:FB:47:2A:36:B2:7C:CA:CE:86:24:A3:6F:39:62:D3:02:03:01:00:01*
Subject Key Identifier	*35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*
Authority Key Identifier	*87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17*
Basic Constraints	*IsCA: true*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS text: [ANF AC emisor de certificados reconocidos conforme la Ley 59/2003 España. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]* *CPS pointer: https://www.anf.es/es/documentos*
CRL Distribution Points	*https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl* *https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl* *ldap://ldap.anf.es:389/cn=ANF_Global_Root_CA_arl.crl,ou=ANF_Global_Root_CA,dc=anf* *DC=anf,CN=ANF_Global_Root_CA_arl.crl,OU=ANF_Global_Root_CA*
Authority Info Access	*http://ocsp.anf.es/spain/AV*
Subject Alternative Name	*http://www.anf.es* *info@anf.es* *OU=" Inscrita en el Ministerio del Interior de España con el numero nacional 171.443", SERIALNUMBER=" G63287510", O=ANF Autoridad de Certificacion, L=Barcelona, STREET=Gran Via de les Corts Catalanes. 996. 08018*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*FB:E0:EC:01:17:9E:8F:99:CC:58:BF:D2:53:8A:B1:1E:75:7D:18:C6:43:7A:8D:C9:65:19:10:F4:45:3C:D4:C5*

X509SubjectName

Subject CN:	*ANF Assured ID CA1*
Subject SERIAL NUMBER:	*G63287510*
Subject E:	*info@anf.es*
Subject OU:	*ANF Autoridad Intermedia de Identidad*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*
Subject ST:	*Barcelona*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-10-28T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

6.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22*

6.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

6.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.2.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.13

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.14

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.15

Description

6.2.5 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificate issued by ANF Assured ID CA1

Name [es] Certificado reconocido emitido por la CA ANF Assured ID CA1

Service digital identities

X509SubjectName

Subject CN:	*ANF Assured ID CA1*
Subject SERIAL NUMBER:	*G63287510*
Subject E:	*info@anf.es*
Subject OU:	*ANF Autoridad Intermedia de Identidad*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*
Subject ST:	*Barcelona*
Subject C:	*ES*

X509SKI

X509 SK I	*NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2018-03-15T01:00:00Z*

6.2.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22*

6.2.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.2.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.2.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.13

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.14

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.15

Description

6.2.6 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificate issued by ANF Assured ID CA1

Name [es] Certificado reconocido emitido por la CA ANF Assured ID CA1

Service digital identities

X509SubjectName

Subject CN: ANF Assured ID CA1

Subject SERIAL NUMBER: G63287510

Subject E: info@anf.es

Subject OU:	*ANF Autoridad Intermedia de Identidad*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*
Subject ST:	*Barcelona*
Subject C:	*ES*

X509SKI

X509 SK I	*NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

6.2.6.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22*

6.2.6.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.2.7 - History instance n.3 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificate issued by ANF Assured ID CA1*

Name [es] *Certificado reconocido emitido por la CA ANF Assured ID CA1*

Service digital identities

X509SubjectName

Subject CN: *ANF Assured ID CA1*

Subject SERIAL NUMBER: *G63287510*

Subject E: *info@anf.es*

Subject OU: *ANF Autoridad Intermedia de Identidad*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*

Subject ST: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-09-15T00:00:00Z*

6.2.7.7 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22*

6.3 - Service (granted): Qualified certificates issued by ANF High Assurance AP CA1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by ANF High Assurance AP CA1*

Name *[es]* *Certificados cualificados emitidos por ANF High Assurance AP CA1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *894242143131763584*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHZzCCBcOgAwIBAgIIDGj8fcSNg4AwDQYJKoZIhvcNAQELBQAwgYAxEjAQBgNVBAUTCUc2MzI4
NzUxMDEbMBkGA1UEAwwSQU5GIFdsb2lhbCBSb290IENBMQswCQYDVQQGEwJFUzEXMBUGA1UECwwO
QU5GIENsYXNlIDEgQ0ExIzAlBgNVBAoMHkFOR0lBIkDXRvcmlkYWQgZGI/gQ2VydGlmaWNhY2lvbyAc
Fw0xNjA1MjAxNTA4MjlaFw0yNjA1MTgxNTA4MjlaMIGaMRIwEAYDVQQFEwlHNjMyODc1MTAxIjAg
BgNVBAMMGUFORiBlaWdoIEFzc3VyYW5jZSBBUCBDQTExCzAJBgNVBAYTAkVTMSowKAYDVQQLDCFB
TkYgQXV0b3JpZGFkIEludGVybWVkaWEgUEtkZSBBUEkxIzAlBgNVBAoMHkFORiBBdXRvcmlkYWQg
ZGI/gQ2VydGlmaWNhY2lvbyCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAISTL35TGPo9
8QbizefyOwLCZO7lHrb4Db1btZr0D6PXksBaA3WRLw/vUIWwLP5+RWVxHBat5vhCehmZxw7bSolc
AxoKvtzmYoKUPt1KzquB/UMlRTOcBGVKJn6boSpFJlRO1GPlRf69gl4M3z75x+P/a4r3CpDvwX3p
4mZZsoWr6aVPpcKs4AG7Tn2dWPuoLQ+9ZN/UQ2iY19QBvfV4JvBBWqOc9L2s0I3mvWGQ6DE8mK+
nlaNFETjfrcXcDPUpAwOAVPIcGb7Wr9ArYNevMmI5qiQMkozH05QBcQNupkdXUgbMYONKMkzMACH
EJpixUjnFrQq6ls3Qsv0E8xfyRrghdHvamsYJN4hlaSNEMct2Xxds5PxIwM9T61eEyAKyWxa6Vtm
hxmzhDmXlzsa2SH+/FDQOzR0Yuvq6Xar8FJQ2wrlekbHH5tuwAmw6qMrtZYOntsVfDIyD1cvp0
OXcid+UFP9dy2HU+Nme65Un7jORNu8FCbnnNB6BNAj+rd+3Ux+0BAWIYOTCoE9mOSmhLPk9DOyBd
2Pi+d9uPeVo2VlkKDLJ3yTWgrdK5E2VkK+V9KVHXMgwIwtoVz21sEFHgs9u8oXOoYz+Pptq5Zs
A51OgJZcRJNzhJCIBHGyq8CDnB4EDBqfdILcy54L8/pv7KGIDXBmmzlmYlaIfVG45xAgMBAAGjggI7
MIICNzAdBgNVHQ4EFgQUkkf90sNhK6nHCac9PjUnUTElbDUwHwYDVR0jBBgwFoAUh/qc31J2dexJ
SiBvW3CWj53vuxcwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwggEcBgNVHSAEggET
MIIBDzCCAQsGBFUdIAAwggEBMIHRBggrBgEFBQcCAjCBxBqBwUFORiBBOyBlbWlzb3IgZGUgY2Vy
dGlmaWNhZG9zIHJlY29ub2NpZG9zIGNvbmZvcm1lIGxhIExlaSA1OSByMDAxLiBlbWFscXVpZXIg
dXNvIGRlIGVzdGUgY2VydGlmaWNhZG8gaW1wbGlyYSBsYSBhY2VwdGFjaW9uIGRlIGxhIENQUyB5
IGRlIGxhcyBsaW1pdGFjaW9uZXMgZGUgcmVzcG9ue2FiaWxpZGFkIGVuIGVzdGFibGVjaWRh
cy4wKwYIKwYBBQUHAgEWH2htdHA6Ly93d3cuYW5mLmVzL2VzL2RvY3VtZW50b3MwewYDVR0fBHQw
cjA3oDWgM4YxaHR0cHM6Ly93d3cuYW5mLmVzL2NybC9BTkZlR2xvYmFsX1Jvb3RfQ0FlYXJsLmNy
bDA3oDWgM4YxaHR0cHM6Ly9jcmwuYW5mLmVzL2NybC9BTkZlR2xvYmFsX1Jvb3RfQ0FlYXJsLmNy
bDA3BggrBgEFBQcBAQQrMCkwJwYIKwYBBQUHMAGGG2h0dHA6Ly9vY3NwLmFuZi5lcy9zcGFpbi9B
VjANBgkqhkiG9w0BAQsFAAOCAgEAGmcx5e0C28mvaQFwS89vFUELfy3P+eoCyjl2hXldyGjDnEY
tsWAgdVcdypdMcMXbspoaSC+HFbWXIb/cWu6yrMSqm+Vljc22jjJT0OZ5KU2VC7yzTsEsGH3Bb6s
UuSzGmdvhParhI+Ed3faSlhOjXM3JSEhSbDPeEZd0du/pWu+tOyHRETS+UbTc+0FagwoApIo0go
5Yz27eshMYe3/R/G6wtz4ybEJVT9VLiOjSjrwAG3oywIW7Vj6SgMVFTXQiJvh6Ipi5bQwM+aw46o
kZwCCxPAWjBI7Vqb5v81UzfIOZ+SBJjRC5PyWkTNJoosv4YJ95aiZpCOgAWNAAzPe14t/ViEqwn
l9OykKMWuPi+8JHrsJA13QOz7Jupk4e6eRCDfqzmIdDQ2WYDJBb0lInJ3nbYLFcPvQPv5OGxbc
jWVsWEj5qskV0KsPz2GXo0Lr0reWkHffcxBtrinLgoSlRMKuI36bZyIkIcmaP63PkICUx/XTfLhL
MC63ctfxUWPONXEsnLL00FAaAFUflI5p67vw0eaLfuaH7A+HYobY6daXpjmdmYWop4n82nNL7vBk
V0gSop6bthQV0zcOTSkhp/Qw3Cllt0JhMVAI7ahq5TiCYqcbOPJPfSpQdhdrSZYXTTot0lWyo68u
3o8Ejz23FGpwvWj+vvGu1Mghomc=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer O: *ANF Autoridad de Certificacion*

Issuer OU: *ANF Clase 1 CA*

Issuer C: *ES*

Issuer CN: *ANF Global Root CA*

Issuer SERIAL NUMBER: *G63287510*

Subject O: *ANF Autoridad de Certificacion*

Subject OU: *ANF Autoridad Intermedia PKde API*

Subject C: *ES*

Subject CN: *ANF High Assurance AP CA1*

Subject SERIAL NUMBER: *G63287510*

Valid from: *Fri May 20 17:08:29 CEST 2016*

Valid to: *Mon May 18 17:08:29 CEST 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:84:93:2F:7E:53:18:FA:3D:F1:06:E2:CD:E7:F2:3B:02:C2:64:EE:E5:1E:B6:F8:0D:BD:5B:B5:9A:F4:0F:A3:D7:92:C0:5A:03:75:91:2F:0F:EF:50:85:B0:2C:FE:7E:45:65:71:1C:16:AD:E6:F8:42:7A:19:99:C7:0E:DB:4A:89:5C:03:1A:0A:BE:DC:E6:62:82:94:3E:DD:4A:CE:AB:81:FD:43:25:45:33:9C:04:65:4A:26:7E:9B:A1:2A:45:24:84:4E:D4:63:C8:45:FE:BD:80:8E:0C:DF:3E:F9:C7:E3:FF:6B:8A:F7:0A:90:EF:C1:7D:E9:E2:66:59:B2:85:AB:E9:A5:4F:A5:C2:AC:E0:01:BB:4E:7D:9D:58:FB:A8:2D:0F:BD:64:DF:D4:43:68:98:D7:D4:01:BD:F1:55:E0:9B:C1:05:6A:8E:73:D2:F6:B3:42:37:9A:F5:86:43:A0:C4:F2:62:BE:9C:86:8D:14:44:E3:B6:F5:DE:0C:F5:29:03:03:80:54:F9:5C:1A:1E:D6:AF:D0:2B:63:73:5E:BC:C9:88:E6:A8:90:E0:CA:33:1F:4E:50:85:03:6E:A6:47:57:27:78:1F:31:83:8D:28:C9:33:30:00:87:10:9A:62:C5:48:E7:16:B4:2A:EA:5B:37:42:CB:F4:13:CC:5F:C9:1A:E0:85:D1:EF:6A:6B:18:24:DE:21:95:A4:8D:10:C7:2D:D9:7C:5D:B3:93:F1:23:03:3D:4F:AD:5E:13:20:0A:C9:6C:5A:E9:5B:66:87:19:B3:84:39:97:97:3B:1A:D9:21:C8:FB:F1:43:40:EC:D1:D1:8B:AF:AB:A5:DA:AF:C1:49:43:6C:2B:95:E9:1B:1C:7E:6D:BB:00:26:C3:AA:8C:AE:D6:58:3A:7B:6C:55:F2:5F:0F:20:F5:72:FA:74:39:77:22:77:E5:05:3F:D7:72:D8:75:3E:36:67:BA:E5:49:FB:8C:E4:4D:BB:C1:42:6E:79:CD:07:A0:4D:02:3F:AB:77:ED:D4:C7:ED:01:01:69:58:39:30:A8:13:D9:8E:4A:68:4B:3E:4F:43:3B:20:5D:D8:F8:BE:77:DB:8F:79:5A:36:56:59:0A:0C:B2:77:C9:35:A0:AD:D2:B9:13:65:64:2B:E5:7D:29:51:D7:32:0C:25:C2:DA:15:CF:6D:6C:10:51:ED:82:CF:6E:F2:85:CE:A1:8C:FF:F8:FA:6D:AB:96:6C:03:9D:4E:80:9D:9C:44:93:73:84:90:AD:04:71:B2:AB:C0:83:9C:1E:04:0C:1A:BA:22:D2:DC:CB:9E:0B:F3:FA:6F:EC:A1:83:5C:19:A6:CC:89:98:95:A1:D5:1B:8E:71:02:03:01:00:01

Subject Key Identifier *92:47:FD:D2:C3:61:2B:A9:C7:09:A7:3D:3E:35:27:51:31:08:6C:35*

Authority Key Identifier *87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17*

Basic Constraints *IsCA: true*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [ANF AC emisor de certificados reconocidos conforme la Ley 59/2003. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]

CPS pointer: http://www.anf.es/es/documentos

CRL Distribution Points

https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl

https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl

Authority Info Access *http://ocsp.anf.es/spain/AV*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4D:C5:4F:4C:5B:DA:C1:95:57:06:6E:32:F6:2F:8C:48:6B:15:5B:00:F5:3D:10:2D:E7:8C:98:EE:61:A2:C3:17*

X509SubjectName

Subject O: *ANF Autoridad de Certificacion*

Subject OU: *ANF Autoridad Intermedia PKde API*

Subject C: *ES*

Subject CN: *ANF High Assurance AP CA1*

Subject SERIAL NUMBER: *G63287510*

X509SKI

X509 SK I	*kkf90sNhK6nHCac9PjUnUTEIbDU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-03-15T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

6.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

6.4 - Service (granted): Qualified certificates issued by ANF High Assurance EV CA1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by ANF High Assurance EV CA1*

Name *[es]* *Certificados cualificados emitidos por ANF High Assurance EV CA1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *458635322224564480*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIRzCCBi+gAwIBAgIIBl1mZUakWQAwDQYJKoZIhvcNAQELBQAwgYAxEjAQBgNVBAUTCUc2MzI4
NzUxMDEbMBkGA1UEAwwSQU5GIEdsb2JhbCBSb290IENBMQswCQYDVQQGEwJFUzEXMBUGA1UECwwO
QU5GIENsYXNlIDEgQ0ExJzAlBgNVBAoMHkFORiBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbjAe
Fw0xNjA1MjAxNDQ4MjRaFw0yNjA1MTgxNDQ4MjRaMIGaMRIwEAYDVQQFEwlHNjMyODc1MTAxIjAg
BgNVBAMMGUFORiBlaWdoIEFzc3VyYW5jZSBFViBDQTExCzAJBgNVBAYTAkVTMSowKAYDVQQLDCFB
TkYgQXV0b3JpZGFkIEludGVyYWVkaWEgVGVjbmljb3MxJzAlBgNVBAoMHkFORiBBdXRvcmlkYWQg
ZGUgQ2VydGlmaWNhY2lvbjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJFFNJ/e0Ade
b4DaRrT6+Gl52TPovOXyzSP/T1PCEI96CTRb/IAxwioLplEfgQvdXcu6/17w8zw6mkRK2X+wcJ6z
GszyvLthtzlHTAE35Tvsicv1AvxvnRotmlalNinFujmcpB0PjglsvgpTqqE5/XRpVaeIHY9Lzp8
1XZP0iHZRRT8Y9vD7urnZ0BWfrYXK0x7IcXAEyYAHQGSHjNLLJbsnxBt4XhNmAHAB8msdCbFbcV3
HT9Tm14BYS6GcY0HLmGVa75dOZHqnxWrypxg4n+cptN+m889g+/jPauJuHG0fQak3GDnvzo1+dkg
FfQnJIloEFNmhuCULfbWUakQIX3O2kQHVuvzX6lktRW6i670Pgg98P+5yIynlWQbcksHMwr/dM+y
+wtSzn2BJUr7nJFQwTsxsw6BJfsDmE42vPwhbrRzRM8ss08/SYoHBpkUEYYRCobJkxZPoWNem/bh2
+gK0226dqDr4i0dkT/FYsOzJjaZdcb4m1AYtpGTrSpnwy1LeRIuKPbEElcPsaS8k0iDeE/DIuJC
rB3ysMAy3j4kkdKTFBGbWFmcNewNDY2AD+z7SlmbyQS6ly+PRotzn6Q3Zogp+m7jDxLh+67QoUgQ
u03sn4X5BbWNEWXYyxXn1X/7cxd/QpBVhT/DWNnPL/uBP/gHjS+cig1u0z+1Yb9FAgMBAAGjggKn
MIICozAdBgNVHQ4EFgQUhr7j+7o/USoRzErcpBe4gsIzngwHwYDVR0jBBgwFoAUh/qe31J2dcxJ
SiBvW3CWj53vuxcwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwggEIBgNVHSAEggEc
MIIBGDCCARQGBFUdIAAwggEKMIHIaBggrBgEFBQcCAjCBzRqBykFORiBBQyBlbWlzb3IgZGUgY2Vy
dGlmaWNhZG9zIHJlY29ub2NpZG9zIGNvbmZvcm1lIGxhIGxlZ2lzbGFjaW9uIGVzcGFub2xhLiBD
dWFscXVpZXIgdXNvIGRlIGVzdGUgY2VydGlmaWNhZG8gaW1wbGljYSBsYSBhY2VwdGFjaW9uIGRl
IGxhIENQUyBSIGRlIGxhcyBsaW1pdGFjaW9uZXMgZGUgcmVzcG9uc2FiaWxpZGFkIGVuIGVsIGVz
dGFiIGVjaWRhcy4wKwYJKwYBBQUHAgEWH2hldHA6Ly95d3cuYW5mLmVzL2RvY3VtZW50b3Mw
gYMGA1UdHwR8MHowO6A5oDeGNWh0dHA6Ly93d3cuYW5mLmVzL2NybC9BTkZfR2xvYmFsX1Jvb3Rf
Q0FlMjAzNl9hcmwuY3JsMDugOaA3hjVodHRwOi8vY3JsLmFuZi5lcy9jcmwvQU5GX0dsb2JhbF9S
b290X0NBXzIwMzZfYXJsLmNybDCBkAYIKwYBBQUHAQEEgYMwgYAwJwYIKwYBBQUHMAGGG2h0dHA6
Ly9vY3NwLmFuZi5lcy9zcGFpbn9BVjBYBggrBgEFBQcwAoZIaHR0cDovL2FuZi5lcy9lcy9jZXI0
aWZpY2F0ZXNfZG93bmxvYWQvQU5GX0dsb2JhbF9Sb290X0NBX1NIQTI1Nl8yMDM2LmNlcjANBgkq
hkiG9w0BAQsFAAOCAgEAaaMSKjUEfaYMQ2tOjQL/EYWsNXTJplsIGBLa17hO8zsRxDqL0iajwm9l
rqOrOJBGRb5Wrtktl2U/+cZ3wVSZzZcx7V7bq+syKQskQo/10RVNEbFiuVOomzA5cgNAMhi1TpZuDP
R5m23x0iNEQXSZHVSoXrA/qRIqiTqdcuxxTZP6CLk79BPbGGmSZkGirT/cFxG5SyTK2ILcMOdYw
2Cs46d5wAnRqphh53t1McA89WTAjYtMryEpuvo4hRxn8qOyrkEHGc/nPk5WG2PW3G/B/cOZu49
2sAzxw6Bao3NHsAH2WjsXz6tGxqHeNipd5wKBLqoNc+U5J963iG7Qpxb2vvxAtPlMZGiguM12Zn
PogjySMEI8yrJ+gyU86oci/XQlkz1u6apbiH/fvpcfpXpQ0Zc3RczwoGa/wM6ksvL6NEXlIwtaDG
nitZejLKXOALZfmp5ncAUG71FaL0nWH6hA/UITDomDnV+oQDx8pQ63E5zgTgamVRz0WlcUNaJK
pbkhQwAbkMQXIA0KF3Xm4jEOL3/6Vvyf1JZgd6QBBLI9dVKGHcYpgU59U1aNRVk9IttHE8xrvB7dD
cdda7y/SmUwTMnHoTTiTKPHprl2FUJw+CrYKcWAUSi2G14eAoO87Ev3jlNCdiEuUK3SHA32ESn1
a2GqE1Tu3GESjvS138s=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer O: *ANF Autoridad de Certificacion*

Issuer OU: *ANF Clase 1 CA*

Issuer C: *ES*

Issuer CN: *ANF Global Root CA*

Issuer SERIAL NUMBER: *G63287510*

Subject O: *ANF Autoridad de Certificacion*

Subject OU: *ANF Autoridad Intermedia Tecnicos*

Subject C: *ES*

Subject CN: *ANF High Assurance EV CA1*

Subject SERIAL NUMBER: *G63287510*

Valid from: *Fri May 20 16:48:24 CEST 2016*

Valid to: *Mon May 18 16:48:24 CEST 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:45:34:9F:DE:D0:07:5E:6F:80:DA:46:B4:FA:F8:69:79:D9:33:E8:BC:E5:F2:CD:23:FF:4F:53:C2:10:8F:7A:09:34:5B:FE:50:31:C1:FA:0B:A4:81:1F:81:0B:DD:5D:CB:BA:FF:5E:F0:F3:3C:3A:9A:44:64:D9:7F:B0:78:9E:B3:1A:CC:F3:C8:BB:61:B7:39:6D:1D:30:04:DF:94:EF:B2:27:2F:D4:0B:F1:BE:74:68:B6:69:5A:20:D8:A7:16:E8:E7:72:90:74:3E:38:25:B2:F8:29:4E:AA:84:E7:F5:D1:A5:56:9E:20:76:3D:2F:3A:7C:D5:76:4F:3A:21:D9:45:14:FC:57:DC:43:EE:EA:E7:67:48:56:7E:B6:17:2B:4C:7B:21:C5:C0:13:25:40:1D:01:92:1F:F8:CD:2C:B2:61:B2:7C:41:B7:85:E1:36:60:07:00:19:AC:74:28:45:6D:C5:77:1D:3F:53:9B:5E:01:61:2E:86:71:8D:07:2E:61:95:6B:BE:5D:39:91:EA:9F:15:AB:CA:9C:60:E2:7F:9C:A6:D3:7E:9B:CF:3D:83:EF:E3:3D:AB:89:B8:71:8E:7D:06:A4:DC:60:E7:BF:3A:09:F9:D9:20:15:F4:27:24:89:68:10:53:66:86:E0:94:2D:F6:D6:51:A9:10:21:7D:CE:DA:44:07:56:EB:F3:5F:A9:64:B5:15:BA:8B:AE:F4:3E:08:3D:F0:FF:B9:CB:5C:A7:95:64:1B:7A:4B:07:33:0A:FF:74:CF:B2:FB:0B:52:9B:60:49:52:BE:E7:24:54:30:4E:CC:6C:C3:A0:49:7E:C0:E6:13:8D:AF:3F:08:5B:AD:1C:D1:33:CB:2C:3B:CF:D2:62:81:C1:A6:45:04:61:84:42:A1:B2:64:C5:93:E8:58:D7:A6:FD:B8:76:FA:02:B4:DB:6E:B8:80:3A:F8:8B:47:71:4F:F1:58:B0:EC:C9:8D:A6:5D:72:1E:26:D4:06:2D:A4:64:EB:4A:9C:2E:FF:22:DE:44:8B:8A:3F:C1:04:95:E3:EC:BB:CE:64:D2:22:43:79:FF:C3:96:E2:42:AC:1D:F2:B0:C0:32:DE:3E:24:91:D2:93:14:11:9B:58:59:9C:35:EC:0D:0D:8D:80:0F:EC:FB:4A:59:9B:C9:04:BA:97:2F:8F:46:8B:73:9F:A4:37:66:88:29:FA:6E:E3:0F:12:E1:FB:AE:D0:A1:48:10:BB:4D:EC:9F:85:F9:05:B5:8D:11:65:D8:CB:15:E7:D5:7F:FB:73:17:7F:42:90:55:85:3F:C3:58:D9:CF:2F:FB:81:3F:F8:07:8D:2F:9C:8A:0D:6E:D3:3F:B5:61:BF:45:02:03:01:00:01

Subject Key Identifier

86:BE:E3:8B:EE:E8:FD:4B:28:47:31:2B:72:90:5E:E2:0B:25:CE:78

Authority Key Identifier

87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

Basic Constraints

IsCA: true

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [ANF AC emisor de certificados reconocidos conforme la legislacion espanola. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]

CPS pointer: http://www.anf.es/es/documentos

CRL Distribution Points

http://www.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl

http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl

Authority Info Access

http://ocsp.anf.es/spain/AV

http://anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

1C:28:A8:C0:09:F2:58:50:B9:15:55:33:D4:A9:A1:4C:53:4B:24:DA:84:75:6E:82:D6:15:0B:50:62:D6:37:04

X509SubjectName

Subject O:

ANF Autoridad de Certificacion

Subject OU:

ANF Autoridad Intermedia Tecnicos

Subject C:

ES

Subject CN:

ANF High Assurance EV CA1

Subject SERIAL NUMBER:

G63287510

X509SKI

X509 SK I

hr7ji+7o/UsoRzErcpBe4gslzng=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-03-15T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

6.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

6.5 - Service (granted): Qualified timestamps issued by ANF High Assurance EV CA1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified timestamps issued by ANF High Assurance EV CA1*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por ANF High Assurance EV CA1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *458635322224564480*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIRzCCBj+gAwIBAgIIBl1mZUakWQAwDQYJKoZIhvcNAQELBQAwgYAxEjAQBgNVBAUTCUc2MzI4
NzUxMDEbMBkGA1UEAwwSQU5GIEdsb2JlbCBSb290IENBMQswCQYDVQQGEwJFUzEXMBUGA1UECwwO
QU5GIENsYXNlIDEgQ0ExJzAlBgNVBAoMHkFORiBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhYQlvbjAe
Fw0xNjA1MjAxNDQ4MjRaFw0yNjA1MTgxNDQ4MjRaMIGaMRIwEAYDVQQFEwlHNjMyODc1MTAxIjAg
BgNVBAMMGUFORiBlaWdoEFzc3VyYWS5ZSBFViBDQTExCzAJBgNVBAYTAkVTMSowKAYDVQQLDCFB
TkYgQXV0b3JpZGFkIEludGVybWVkaWEgVGVjbmljb3MxJzAlBgNVBAoMHkFORiBBdXRvcmlkYWQg
ZGUgQ2VydGlmaWNhY2lvbjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJFFNJ/e0Ade
b4DaRrT6+Gl52TPovOXyzSPT1PCEJ96CTRb/lAxwiIoLplEfgQvdXcu6/17w8zw6mkRKZX+wel6z
GszzyLIhtzlHTTAE35Tvsicv1AvxvnRotmlaINinFujncpB0PjglsvgpTqqE5/XRpVaeHY9Lzp8
1XZPOtHZRRT8Y9xD7tarnZ0lbWtFYXK0x7lcXAEyYAHQGSIl/jNLLlhsnxBt4XhNmAHAB3msdChFbcV3
HT9Tm14BYS6GcY0HLmGVa75dOZHqnxWrypxg4n+cptN+m889g+/jPauJuHGOfQak3GDnvzoJ+dkg
FfQnJIloEFNmhuCULfbWUakQIX3O2kQHVuvzX6ktRW6i670Pgg98P+5y1ynIWQbeksHMwr/dM+y
+wtSm2BJUr7nJFQwTsxsw6BJfsDmE42vPwhbrRzRM8ssO8/SYoHBpkUEYYRCobJkxZPoWNem/bh2
+gK0226HgDr4t0dxT/FYsOcfjaZdcb4m1AYtpGTrSpnw/yLeRIuKPbEEIcPsaSSk0tJDcf/DIuIC
rB3ysMAy3j4kkdKTFBGbWFmcNewND Y2AD+z7SlmbyQS6ly+PRotzn6Q3Zogp+m7jDxLh+67QoUgQ
u03sn4X5BbWNEWXYyxXn1X/7cxd/QpBVhT/DWNnPL/uBP/gHJs+cig1u0z+1Yb9FAgMBAAGjggKn
M1ICozAdBgNVHQ4EFgQUhr7j+7oUsoRzEcpBe4gslzmgwHwYDVR0jBBgwFoAUh/qe31J2dexJ
Si8vW3CWj55vuxcwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwggEIBgNVHSAEggEc
MIIBGDCCARQGBFUdIAAwggEKMIHaBggrBgEFBQcCAjCBzRqBykFORiBBQyBlbWlzb3IgZGUgY2Vy
dGlmaWNhZG9zIHJlY29ub2NpZG9zIGNvbmZvcm1lIGxhIGxlZ2lzbGFjaW9uIGVzcGFub2xhLiBD
dWFscXVpZXIgdXNvIGRlIGVzdGUgY2VydGlmaWNhZGBgaW1wbGlyYSBsYSBbY2VwdGFjaW9uIGRl
IGxhIENQUybSIGRlIGxhcyBsaW1pdGFjaW9uZXMgZGUgcmVzcG9uc2FiaWxpZGFkIGVsIGVz
dGFibGVjaWRhcy4wKwYIKwYBBQUHAgEWH2h0dHA6Ly93d3cuYW5mLmVzL2NybC9BTkZlR2xvYmFsX1Jvb3Rf
Q0FfMjAzNl9hcmwuY3JsMDugOaA3hjVodHRwOi8vY3JsLmFuZi5lcy9jcmwvQU5GX0dsb2JhbF9S
b290X0NBXzIwMzZfYXJsLmNybDCBkAYIKwYBBQUHAQEEgYMwgYAwJwYIKwYBBQUHMAGGG2h0dHA6
Ly9vY3NwLmFuZi5lcy9zcGFpb9BVjB VBggrBgEFBQcwAoZIaHR0cDovL2FuZi5lcy9lcy9pZXI0
aWZpY2F0ZXNfZG93bmxvYWQvQU5GX0dsb2JhbF9Sb290X0NBX1NIQT1Nl8yMDM2LmNlcjANBgkq
hkiG9w0BAQsFAAOCAgEAaaMSKjUEfaYMQ2tOjQL/EYWsNXTJplstGBLa17bO8zsRxDqL0iajwm9l
rqQrOJBGRb5Wrtkt0ZU+eZ3wVSZzZcx7V7bq+syKQskQo/10RVNEbFiuVOmzzAScgeNAMhi7pZuDP
R3m23xIINEQXS2HV5oXcA/qRIqiTqddcuxxTZP6CLk79BPbGGmSZkGirT/cfxGS5yTK2ILcMOdYw
2Cs46d5wAnRqnhb53t1McA89WTAijYtMryEpuvo4hRxn8qOjrkEHGe/nPk5WG2PW3G/B/cOZu49
2sAzxw6Bao3NHsAH2WjsXz6tGxqHeNipd5wKBLqoNc+U5J963iIG7Qpxb2vvxAtPlMZGiguM12Zn
PogjySMEl8yrJ+gyU86oci/XQlkzTu6apbsH/tvpcfpXpQ0Zc3RczwoGa/wM6ksvL6NEXIlwtaDG
nitzZcjLKXOALZfmp5ncAUG71FaLOnWH6bA/UITDomDmV+oQDz8tpQ63L5zgTgamVRc0WlcUNaJK
pbkhQwAbkMQXIA0KF3Xm4jEOL36Vvyf1JZgd6QBBLI9dVKGHcYpgU59U1aNRVk9ltHE8xrvB7dD
cdda7y/SmIJwTMnHoTTiTKPHpri2FUJw+CrYKcWAUSi2G14eAoO87Ev3jlNCdiEuUK3SHA32ESn1
a2GqE1Tu3GESjvS138s=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *ANF Autoridad de Certificacion*

Issuer OU:	*ANF Clase 1 CA*
Issuer C:	*ES*
Issuer CN:	*ANF Global Root CA*
Issuer SERIAL NUMBER:	*G63287510*
Subject O:	*ANF Autoridad de Certificacion*
Subject OU:	*ANF Autoridad Intermedia Tecnicos*
Subject C:	*ES*
Subject CN:	*ANF High Assurance EV CA1*
Subject SERIAL NUMBER:	*G63287510*
Valid from:	*Fri May 20 16:48:24 CEST 2016*
Valid to:	*Mon May 18 16:48:24 CEST 2026*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:45:34:9F:DE:D0:07:5E:6F:80:DA:46:B4:FA:F8:69:79:D9:33:E8:BC:E5:F2:CD:23:FF:4F:53:C2:10:8F:7A:09:34:5B:FE:50:31:C1:FA:0B:A4:81:1F:81:0B:DD:5D:CB:BA:FF:5E:F0:F3:3C:3A:9A:44:64:D9:7F:B0:78:9E:B3:1A:CC:F3:C8:BB:61:B7:39:6D:1D:30:04:DF:94:EF:B2:27:2F:D4:0B:F1:BE:74:68:B6:69:5A:20:D8:A7:16:E8:E7:72:90:74:3E:38:25:B2:F8:29:4E:AA:84:E7:F5:D1:A5:56:9E:20:76:3D:2F:3A:7C:D5:76:4F:3A:21:D9:45:14:FC:57:DC:43:EE:EA:E7:67:48:56:7E:B6:17:2B:4C:7B:21:C5:C0:13:25:40:1D:01:92:1F:F8:CD:2C:B2:61:B2:7C:41:B7:85:E1:36:60:07:00:19:AC:74:28:45:6D:C5:77:1D:3F:53:9B:5E:01:61:2E:86:71:8D:07:2E:61:95:6B:BE:5D:39:91:EA:9F:15:AB:CA:9C:60:E2:7F:9C:A6:D3:7E:9B:CF:3D:83:EF:E3:3D:AB:89:B8:71:8E:7D:06:A4:DC:60:E7:BF:3A:09:F9:D9:20:15:F4:27:24:89:68:10:53:66:86:E0:94:2D:F6:D6:51:A9:10:21:7D:CE:DA:44:07:56:EB:F3:5F:A9:64:B5:15:BA:8B:AE:F4:3E:08:3D:F0:FF:B9:CB:5C:A7:95:64:1B:7A:4B:07:33:0A:FF:74:CF:B2:FB:0B:52:9B:60:49:52:BE:E7:24:54:30:4E:CC:6C:C3:A0:49:7E:C0:E6:13:8D:AF:3F:08:5B:AD:1C:D1:33:CB:2C:3B:CF:D2:62:81:C1:A6:45:04:61:84:42:A1:B2:64:C5:93:E8:58:D7:A6:FD:B8:76:FA:02:B4:DB:6E:B8:80:3A:F8:8B:47:71:4F:F1:58:B0:EC:C9:8D:A6:5D:72:1E:26:D4:06:2D:A4:64:EB:4A:9C:2E:FF:22:DE:44:8B:8A:3F:C1:04:95:E3:EC:BB:CE:64:D2:22:43:79:FF:C3:96:E2:42:AC:1D:F2:B0:C0:32:DE:3E:24:91:D2:93:14:11:9B:58:59:9C:35:EC:0D:0D:8D:80:0F:EC:FB:4A:59:9B:C9:04:BA:97:2F:8F:46:8B:73:9F:A4:37:66:88:29:FA:6E:E3:0F:12:E1:FB:AE:D0:A1:48:10:BB:4D:EC:9F:85:F9:05:B5:8D:11:65:D8:CB:15:E7:D5:7F:FB:73:17:7F:42:90:55:85:3F:C3:58:D9:CF:2F:FB:81:3F:F8:07:8D:2F:9C:8A:0D:6E:D3:3F:B5:61:BF:45:02:03:01:00:01*
Subject Key Identifier	*86:BE:E3:8B:EE:E8:FD:4B:28:47:31:2B:72:90:5E:E2:0B:25:CE:78*
Authority Key Identifier	*87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17*
Basic Constraints	*IsCA: true*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS text: [ANF AC emisor de certificados reconocidos conforme la legislacion espanola. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]* *CPS pointer: http://www.anf.es/es/documentos*
CRL Distribution Points	*http://www.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl* *http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl*
Authority Info Access	*http://ocsp.anf.es/spain/AV* *http://anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1C:28:A8:C0:09:F2:58:50:B9:15:55:33:D4:A9:A1:4C:53:4B:24:DA:84:75:6E:82:D6:15:0B:50:62:D6:37:04*

X509SubjectName

Subject O:	*ANF Autoridad de Certificacion*
Subject OU:	*ANF Autoridad Intermedia Tecnicos*
Subject C:	*ES*
Subject CN:	*ANF High Assurance EV CA1*
Subject SERIAL NUMBER:	*G63287510*

X509SKI

X509 SK I	*hr7ji+7o/UsoRzErcpBe4gslzng=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-03-15T01:00:00Z

6.6 - Service (withdrawn): Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

Service type description	*[en]*	*undefined.*
	[es]	*undefined.*

Service Name

Name	*[en]*	*Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION*
Name	*[es]*	*Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor ANF AUTORIDAD DE CERTIFICACION*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*996613180148035949*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIOyDCCDLCgAwIBAgIIDdSuaDUyMW0wDQYJKoZIhvcNAQELBQAwggEhMQswCQYDVQQGEwJFUzES
MBAGA1UECAwJQmFyY2Vsb25hMVgwVgYDVQQHDE9CYXJjZWxvbmEgKHN0ZSBjdXJvZW50IGFkZHJl
c3MgYXQgaHR0cDovL3d3dy5hbmYuZXMvZXMvYWRkcmVzY1kaXlIY2Npb24uaHRtbCApMScwJQYD
VQQKDB5BTkYgQXV0b3JpZGFkIGRlIENlcnRpZmlqYWNpb24xLjAsBgNVBAsMJUFORiBBdXRvcmlk
YWQgSW50ZXJlZWRpYSBkZSBJZGVudGlkYWQxGjAYBgkqhkiG9w0BCQEWC2luZm9AYW5mLmVzMRIw
EAYDVQQFEwlHNjMyODc1MTAxGzAZBgNVBAMMEkFORiBBc3N1cmVkIEIEIENBMTAeFw0xODEyMjQx
MDAzMTFaFw0yMDEyMjMxMDAzMTFaMIB5TEXMBIGA1UEBQwOVE0ORVNHNjMyODc1MTAxKTAnBgNV
BAsMIENlcnRpZmlqYWRvIGRlIFNlbGxvIEVsZWN0cm9uaWNvMyMGPMIGMBgNVBA0MgYRDYXJnbzpQ
UkVTSURFTiRFIC5JT1NDUkIQQ0nDk046IFJFRy4gOVNPQ0lBQ0lPTkVTIERFTCBNSU5JU1RFUkIP
IERFTCBJTlRFUkIPUi4gR1JVUE8gMcK6LCBTRUMuIDHHCqiwgTIVNL1AxNzE0NDMuIEZFQ0hBOiAx
Mi4wMS4yMDA1LAxEzARBgNVBAwMCIBSRVNlRFEVOVEUxOTA3BgNVBAoMMEFORiBBVVRPUkIEQUQg
REUgQOVSVElGSUNBQ0lPTiBBU09DSUFDSU9OIEFORiBBQzEhMB8GA1UEBAwYREIBWiBWSUxDSEVT
IC0gMzcyNzEzODdXMRIwEAYDVQQqDAIGTE9SRU5DSU8xJTAjBgkqhkiG9w0BCQEMFnNlcnZpY2lv
dGVjbmljb0BhbmYuZXMxDzANBgNVBAcMBk1BRFJlRDEPMA0GA1UECAwGTUFEUkIEMQswCQYDVQQG
DAJFUzEwMC4GA1UEAwwnQU5GIEFVVE9SSUIRBCBERSBDRVJUSUZQOFDSU9OICBiTkYgQUMpMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqKCAFZ5LrCAn/a33LD/YqQfZs0vCMKY9/kvy
M1Gx7Ir+08MIyoEZbQEe9I01JZY6UA8lh98UL WpyUhOea0M1vnCRoNzDmyYCJuFWlXpyvRurSKN
Zy2bWW3n22VKylujt4zgT7sGlvXekVHZhizWoE4NpvxNtnILsUOm T5chdI3l+FtWsAK6gIVO401+o
pb8RkLZrcekzPWmrxW3xvKZrsGb65tgsSFcfpsgIuwSY8dWYOQYTJRxJvW0tPTWtka7eWsoalO
Dh4kflh7SOZFxOrGYbaaIdIxGeCkLDyhzxdy7wDqH2fAcT/p5u0Pa4tleuIW9F/McTbq2aS/lENtN
ZQIDAQABo4IOjCCCCDYwDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBPAwgY4GCCsGAQUFBwEB
BIGBMH8wJwYIKwYBBQUHMAGGG2h0dHA6Ly9vY3NwLmFuZi5lcy9zcGFpb9BVjBUBggrBgEFBQcw
AoZIaHR0cDovL3d3dy5hbmYuZXMvZXMvY2VvdGlmaWNhdGVzX2Kvd25ub2Fk1L0FOR9Bc3N1cmVk
X0lEX0NBMV9TSEsyNTYuY2VyMEUGA1UdHwQ+MDwwOqA4oDaGNGh0dHBzOi8vd3d3LmFuZi5lcy9j
cmwvQU5GX0Fzc3VyZWRlSURfQ0ExX1NlQT11Ni5jcmwwggH0BgNVHQkEggHrMIIB5zAdBgNVBA8x
FhMUUHJpdmF0ZSBPcmdhbmI6YXRpb24wFwYLKwYBBAGCNzwCAQExCBMGTWFkcmlkMBcGCysGAQQB
gjc8AgECMQgTBk1hZHJpZDAtBgorBgEEAYGPHIRYMRET0ifSTUQgd4zLjUuMS43MDAWBgorBgEE
AYGPHB4BMQgTBkVzcGJtcYTBVBgorBgEEAYGPHAoKATFGE0RodHRwczovL3RvbWNhdDJlaYW5mLmVz
L2NsaWVudGVlYXJjaGl2b193cy9wb2RlcmVzLzExOTgxNDQ5OC04OT4ODc2NDAjBgNVBAkxHBMa
UEFTRU8gREUgTEEgQ0FTVEVMTEFOQSwgNzkwJwYKKwYBBAGBjxwoATEZExdDRVJUSUZJQ0FETyBD
VUFMSUZJQ0FETzAUBgorBgEEAYGPHCkBMQYTBDEwMDAwDgYDVQQRMQcTBT14MDQ2MBoGCisGAQQB
gY8cWwExDBMKQXNvYZlhY2rzbjASBgNVBCoxCxMJRkxPUkVOQ0lPMCEGA1UEBDEaExhEzLFaFZJ
TENIRVMgLSAzNzI3MTM4N1cwGAYKKwYBBAGBjxwqATEKEwgwMDAtMDAwMDAjBgNVBAkxHBMaUEFT
RU8gREUgTEEgQ0FTVEVMTEFOQSwgNzkwgZAGCCsGAQUFBwEDBIGDMIGAMAoGCCsGAQUFBwsCMBMG
BgQAjkYBBjAJBgcEAISGAQYCMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wFQYGBACORgECMAsTA0VV
UgIBAQIBAzAkBgYEAI5GAQUwGjAVFhJodHRwczovL2FuZ5lcy9lb8TAmVuMAkGBwQAr+xJAQIw
ggGNBgNVHREEggGEMIIBgIEWc2VydmljaW90ZWNuaWNvQGFuZi5lc6AXBgorBgEEAYGPHB0EDAkz
Nzl3MTM4N1egFwYKKwYBBAGBjxwKAQwJRkxPUkVOQ0lPoCEGCisGAQQBgY8cCgMME1ZJTENlRVMg
LSAzNzI3MTM4N1egJAYKKwYBBAGBjxwdBQwWc2VydmljaW90ZWNuaWNvQGFuZi5lc6ATBgorBgEE
AYGPHB0CDAVEwd1BWqAXBgorBgEEAYGPHAoEIAKzNzI3MTM4N1egFwYKKwYBBAGBjxwdAQwJRkxP
UkVOQ0lPoCEGCisGAQQBgY8cHQMME1ZJTENlRVMgLSAzNzI3MTM4N1egEwYKKwYBBAGBjxwKAgwF
RMONQVggJAYKKwYBBAGBjxwKBwwWc2VydmljaW90ZWNuaWNvQGFuZi5lc6AuBgNVBAMM0FORiBB
VVRPUkIEQUQgREUgQ0VSVEIGSUNBQ0lPTiAoQU5GIEFDKaAWBgNVBAUMD1RJTkVTLUc2MzI4NzUx
MDAhBgkrBgEEAYGPHBMEFAwSMTE5ODE0NDk4LTg5Mjg4Nzk0MDIBMwYDVR0OBIIBKgSCASYwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCxoIAVnkusICl9rfcsP9jpB9mzS8lwpj3+S/Iz
UbHsiv7TwwjKgRltAR72XTUlljpQB/yWH5xQtanJSE55trQzW+cJGg3MObJgIm4VaVenK9G6tIo1n
LZtZbefhZUr1ri6PjOBPuwaW9d6RUdmGLNagTg2m/E22eguxQ6ZPlyF0jcX4Vf9awArqCVU7jTX6in
yFGRmtx6SPE/9avvFbIO8pmuwZvrm2CzkV4mmyDW78Jjx1Zg5BhMlHEm9bSs9NauRrv95ayhqU4O
HiR8iHSkXE6sZhtpobIhEZ4KQsPKHPF3LvAOnZ8BxP+nmYQ9n2V659b0X8wfurZpL+UQ2ilI
AgMBAAEwMQYDVR0lBCowKAYIKwYBBQUHAwEGCCsGAQUFBwMCBggrBgEFBQcDAwYIKwYBBQUHAwQw
UAYKKwYBBAGBjxwvAQRCDEBINTY1ZjAzYml2ODc5MzM5NTNlNTk4OTcyYThhZmIxODJmOWI3MzY3
MjYyZDZmMjdjOTQ1ODJkOGUyNWFhZjc2MB8GA1UdIwQYMBaAFDUuLeYpHL+L2Up8nvgIUlRxk89
MCcGCXqGAQQBgY8cEwEEGQwXNTAwMgtMzU5NzQ4NDhzMDgzNjE1MzYwgfgGA1UdIASB8DCB7TCB
3wYMKwYBBAGBjxwZAQEBMIHOMCgGCCsGAQUFBwIBFhxodHRwOi8vd3d3LmFuZi5lcy9kb2N1bWVu
dG9zMIGhBggrBgEFBQcCAjCBlAyBkUNlcnRpZmlqYWRvIGNvbmZvcm1llGEgbGEgbGVnaXNsYWNp
w7NuIGRlIGZpcm1hIGVsZWN0cSOzbmlJYS4gOW50ZXMgZGUgYWNlcHRhcmxvIGNvbXBydWVvZSBp
bnRlZ3IpZGFkLCBaW1pdGFjaW9uZXMsIHZpZ2VuY2lhIHkgdXNvcyBhdXRvcmlkYWRvcy4wCQYH
BACL7EABATANBgkqhkiG9w0BAQsFAAOCAgEAcC6Zu5AWXNS1zTq3QvLecvkun6gi55y45nP6WUnq
XKm0eaM9s46cHBYLKM8vMec+zyh1ul7lU3GVr+4dshyYBuD/AmpBbN7dYTQYiyq2pFbFiaVdc6HT
HtNpn4wsSdA1bsjCAob2lHu3ibl+IObFDUxRrWWv1Quvznwaxas2Y7X6Z2uBozeE88ds7rrdVid
nGJqqQNX6eFdQIcKQTVCyxnUHE3WGytdIYCXpBy2lneFoH7IIg92G1J6DMRJwgwvNPjkXDimrl
ce25WMJpKWDCawYgiQZSbYWj7xEjNqynWOTBvhzf6yAuaYmhR8B+ceYpfuO3W4Lhv86wznqNqTXn
xX94XZPNTL/k8Mvm1F4Ks2o26i9E7xc9wp5afV27fZQpQFC4Z3qLIZUzM2RyPP/nN1Sit+B6BQaK
esI50xpk7RHEWBEN8AF3AXtuIg7AZ8+O0cASXexszuCUQFztkqEPPPsDikmGLnxnUYV66/kvIt2P
ZME3ybm+stq2kuo7ump/6bnNj9NOzH1wn8C/KWSoib1EBwTV3UWQuIM3BcsggDRXVqZ08F3alcT
2nEIoIB3L9zNKWAK2BLusskiRMZvTMoCogKaf8WKc5JgaCYNdPFiiRnC24PvBaH4TSG3b0XMaEiJ
pYVCthiQdITLgaOACyu8IjQOYSrVz+S4ors=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF Assured ID CA1*

Issuer SERIAL NUMBER: *G63287510*

Issuer E: *info@anf.es*

Issuer OU: *ANF Autoridad Intermedia de Identidad*

Issuer O: *ANF Autoridad de Certificacion*

Issuer L: *Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*

Issuer ST: *Barcelona*

Issuer C: *ES*

Subject CN: *ANF AUTORIDAD DE CERTIFICACION (ANF AC)*

Subject C: *ES*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject E: *serviciotecnico@anf.es*

Subject GIVEN NAME: *FLORENCIO*

Subject SURNAME:	*DIAZ VILCHES - 37271387W*
Subject O:	*ANF AUTORIDAD DE CERTIFICACION ASOCIACION ANF AC*
Subject T:	*PRESIDENTE*
Subject 2.5.4.13:	*Cargo:PRESIDENTE .INSCRIPCIÓN: REG. ASOCIACIONES DEL MINISTERIO DEL INTERIOR. GRUPO 1º, SEC. 1ª, NUM. 171443. FECHA: 12.01.2004.*
Subject OU:	*Certificado de Sello Electronico*
Subject SERIAL NUMBER:	*TINESG63287510*
Valid from:	*Mon Dec 24 11:03:11 CET 2018*
Valid to:	*Wed Dec 23 11:03:11 CET 2020*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:A0:80:15:9E:4B:AC:20:27:FD:AD:F7:2C:3F:D8:A9:07:D9:B3:4B:C2:30:A6:3D:FE:4B:F2:33:51:B1:EC:8A:FE:D3:C3:08:CA:81:19:6D:01:1E:F6:5D:35:25:96:3A:50:07:FC:96:1F:7C:50:B5:A9:C9:48:4E:79:AD:0C:D6:F9:C2:46:83:73:0E:6C:98:08:9B:85:5A:55:E9:CA:F4:6E:AD:22:8D:67:2D:9B:59:6D:E7:DB:65:4A:C8:8B:A3:E3:38:13:EE:C1:A5:BD:77:A4:54:76:61:8B:35:A8:13:83:69:BF:13:6D:9C:82:EC:50:E9:93:E5:C8:5D:23:79:7E:15:F5:AC:00:AE:A0:95:53:B8:D3:5F:A8:A7:C8:51:91:9A:DC:7A:48:F1:3F:F5:A6:AF:15:B7:C6:F2:99:AE:C1:9B:EB:9B:60:B3:91:5E:26:9B:20:D6:EC:12:63:C7:56:60:E4:18:4C:94:71:26:F5:B4:AC:F4:D6:AE:46:BB:FD:E5:AC:A1:A9:4E:0E:1E:24:7C:88:7B:48:E6:45:C4:EA:C6:61:B6:9A:21:D2:71:19:E0:A4:2C:3C:A1:CF:17:72:EF:00:EA:1F:67:C0:71:3F:E9:E6:ED:0F:6B:8B:65:7A:E7:D6:F4:5F:CC:09:BA:B6:69:2F:E5:10:DB:4D:65:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Info Access	*http://ocsp.anf.es/spain/AV* *http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer*
CRL Distribution Points	*https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl*
Subject Directory Attributes	*2.5.4.15 Private Organization* *1.3.6.1.4.1.311.60.2.1.1 Madrid* *1.3.6.1.4.1.311.60.2.1.2 Madrid* *1.3.6.1.4.1.18332.600 ARMD v.3.5.1.70* *1.3.6.1.4.1.18332.30.1 España* *1.3.6.1.4.1.18332.10.10.1 https://tomcat2.anf.es/cliente_archivo_ws/poderes/119814498-89288764* *2.5.4.9 PASEO DE LA CASTELLANA, 79* *1.3.6.1.4.1.18332.40.1 CERTIFICADO CUALIFICADO* *1.3.6.1.4.1.18332.41.1 1000* *2.5.4.17 28046* *1.3.6.1.4.1.18332.91.1 Asociación* *2.5.4.42 FLORENCIO* *2.5.4.4 DÍAZ VILCHES - 37271387W* *1.3.6.1.4.1.18332.42.1 000-0000* *2.5.4.9 PASEO DE LA CASTELLANA, 79*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

id_etsi_qcs_LimiteValue

Value: 1000

Currency: EUR

Subject Alternative Name

serviciotecnico@anf.es

Subject Key Identifier

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:A0:80:15:9E:4B:AC:20:27:FD:AD:F7:2C:3F:D8:A9:07:D9:B3:4B:C2:30:A6:3D:FE:4B:F2:33:51:B1:EC:8A:FE:D3:C3:08:CA:81:19:6D:01:1E:F6:5D:35:25:96:3A:50:07:FC:96:1F:7C:50:B5:A9:C9:48:4E:79:AD:0C:D6:F9:C2:46:83:73:0E:6C:98:08:9B:85:5A:55:E9:CA:F4:6E:AD:22:8D:67:2D:9B:59:6D:E7:DB:65:4A:C8:8B:A3:E3:38:13:EE:C1:A5:BD:77:A4:54:76:61:8B:35:A8:13:83:69:BF:13:6D:9C:82:EC:50:E9:93:E5:C8:5D:23:79:7E:15:F5:AC:00:AE:A0:95:53:B8:D3:5F:A8:A7:C8:51:91:9A:DC:7A:48:F1:3F:F5:A6:AF:15:B7:C6:F2:99:AE:C1:9B:EB:9B:60:B3:91:5E:26:9B:20:D6:EC:12:63:C7:56:60:E4:18:4C:94:71:26:F5:B4:AC:F4:D6:AE:46:BB:FD:E5:AC:A1:A9:4E:0E:1E:24:7C:88:7B:48:E6:45:C4:EA:C6:61:B6:9A:21:D2:71:19:E0:A4:2C:3C:A1:CF:17:72:EF:00:EA:1F:67:C0:71:3F:E9:E6:ED:0F:6B:8B:65:7A:E7:D6:F4:5F:CC:09:BA:B6:69:2F:E5:10:DB:4D:65:02:03:01:00:01

Extended Key Usage

id_kp_codeSigning - id_kp_clientAuth - id_kp_serverAuth

Authority Key Identifier

35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D

Certificate Policies

Policy OID: 1.3.6.1.4.1.18332.25.1.1.1

CPS pointer: http://www.anf.es/documentos

CPS text: [Certificado conforme a la legislación de firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.]

Policy OID: 0.4.0.194112.1.1

Key Usage:

digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment

Thumbprint algorithm:

SHA-256

Thumbprint:

B1:14:56:6D:66:73:7E:AC:6F:1C:A1:AA:16:C0:0F:51:89:69:A2:C4:4C:A6:D8:6D:8F:4F:97:EE:A2:41:C8:E9

X509SubjectName

X509SKI

X509 SK I

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqKCAFZ5LrCAn/a33LD/YqQfZs0vCMKY9/kvyM1Gx7Ir+08MIyoEZbQEe9l01JZY6UAf8lh98ULWpyUhOea0M1vnCRoNzDmyYCJuFWlXpyvRurSKNZy2bWW3n22VKyIuj4zgT7sGlvXekVHZhizWoE4NpvxNtnILsUOmT5chdI3l+FfWsAK6glVO401+op8hRkZrcekjxP/WmrxW3xvKZrsGb65tgs5FeJpsg1uwSY8dWYOQYTJRxJvW0rPTWrka7/eWsoalODh4kfIh7SOZFxOrGYbaaIdJxGeCkLDyhzxdy7wDqH2fAcT/p5u0Pa4tleufW9F/MCbq2aS/lENtNZQIDAQAB

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-01-26T01:00:00Z

6.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.6.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q*

Service Name

Name	*[en]*	*Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION*
Name	*[es]*	*Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor ANF AUTORIDAD DE CERTIFICACION*

Service digital identities

X509SubjectName

X509SKI

X509 SK I

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqKCAFZ5LrCAn/a33LD/YqQfZs0vCMKY9/kvyM1Gx7Ir+08MIyoEZbQEe9l01JZY6UAf8lh98ULWpyUhOea0M1vnCRoNzDmyYCJuFWlXpyvRurSKNZy2bWW3n22VKyIuj4zgT7sGlvXekVHZhizWoE4NpvxNtnILsUOmT5chdI3l+FfWsAK6glVO401+op8hRkZrcekjxP/WmrxW3xvKZrsGb65tgs5FeJpsg1uwSY8dWYOQYTJRxJvW0rPTWrka7/eWsoalODh4kfIh7SOZFxOrGYbaaIdJxGeCkLDyhzxdy7wDqH2fAcT/p5u0Pa4tleufW9F/MCbq2aS/lENtNZQIDAQAB

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-02-18T01:00:00Z*

6.6.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.7 - Service (withdrawn): Qualified certificates issued by ANF High Assurance Server CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by ANF High Assurance Server CA*
Name	*[es]*	*Certificados cualificados emitidos por ANF High Assurance Server CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *99659964253702882*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHhDCCBWygAwIBAgIIAWIQNZ+riuIwDQYJKoZIhvcNAQELBQAwgYQxEjAQBgNVBAUTCUc2Mzl4
NzUxMDELMAkGA1UEBhMCRVMxJzAlBgNVBAoTHkFORiBBdXRvcmlkYWQgZGl.lgQ2VydGlmaWNhY2lv
bjEUMBIGA1UECxMLQU5GIENBIEJhaXoxIjAgBgNVBAMTGUFORiBTZWN1cmUgI2VydmVyIFJvb3Qg
Q0EwHhcNMTkwOTA1MTYzNTQ0WhcNMjkwOTAyMTYzNTQ0WjCBnTESMBAGA1UEBRMJRzYzMjg3NTEw
MQswCQYDVQQGEwJFUzEnMCUGA1UECbMcQU5GIEF1dG9yaWRhZCBlZSBDZXJ0aWZpY2FjaW9uMSow
KAYDVQQLEyFBTkYgQXV0b3JpZGFkIGludGVybWVkaWEgdGVjbmljb3MxJTAjBgNVBAMTHEFORiBI
aWdoIEZc1VyYW5jZSBTZXJ2ZXIgQOEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDd
qMviQvX9BJ8mepPFLpQAiDimNZb907XKd/bDbtHQVD/TjlgAWb2tDUzj0/KmVqV/q5AJpbLm3TF
EtgzALDIv7zTDplg9M/yHOY6gyQTso5xvBKcMyFNBc+L8QDIRd7tiZIB8DUPGStiknJjsp9j7acx
iMzp2xtbGL+kIXYdBtXZRGqqE8T8+thMcd2QiRry0xISa06NCBV1xzDSbmFC11HzbD0LXl/Uaoil
5UNi9pKFio4PgMoNAFfaaUhKZR4jTihaVUzrV8YdWgDGjD0IbAQCOACuSNq2Q6U+9WLwTbD4Eex
VZjHoBUK/TxXle56caAfEbrPmS6cSpWe8A1LPbHnqhm8isIk9cN7E+HdyLIX3jPLuibdJWxLDzse
T9Tjxsy8nmyxQ4V+ByAh/BAus3gJPJSM7y9LZ2frEUJOBu3sIG+g2cI1IoQKY6z25jD17SitR+if
W39nmYSXBvfVjoroLYwOZaIYA2lwZSFZ2WcUpvXRucatIlHqIyGvV+rylmJizpbXOwGrnA8sN4/
G+0cMzk8PpcvkSKcpl9mrIM3waKJ96GWUEDTzNvafjnN2XiAvwa4Nvdyx/0lgfz7zg1gKyGr3e5IL
1DcAY3uzxJ0ZxmQ/iNphtDIaeLhO4UrgeSiP0ZwjQ3Nvl6gmhY53Jggo41yrz+fUSlfahVHzQID
AQABo4IB3TCCAdkwHwYDVR0jBBgwFoAUnF/QbGOjX5PKk5glRYyHpSxcwTcwHQYDVR0OBBYEFJS6
+u4i+jlcyvV3txmvEvCabEcrMA4GA1UdDwEB/wQEAwIBhjAnBgNVHSUEIDAeBggrBgEFBQcDAQYI
KwYBBQUHAwIGCCsGAQUFBwMDMH8GA1UdIwR4MHYwOaA3oDWGM2hhdHAsLy9cmwuYW5mLmVzL2Ny
bC9BTkZTZWN1cmVTZXJ2ZXJSb290Q0EtYXJsLmNybDA5oDegNYYzaHR0cDovL3d3dy5hbmYuZXMv
Y3JsL0FORlNlY3VyZVNlcnZlcIJvb3RDQS1hcmwuY3JsMEAGA1UdIAQ5MDcwNQYEVR0gADAtMCsG
CCsGAQUFBwIBFh9odHRwOi8vd3d3LmFuZi5lcy9lcy9kb2N1bWVudG9zMIGJBggrBgEFBQcBAQR9
MHswJwYIKwYBBQUHMAGGG2h0dHA6Ly9vY3Nwc.mFuZi5lcy9zcGFpbi9BVjBQBggrBgEFBQcwAoZE
aHR0cDovL3d3dy5hbmYuZXMvZXMvY2VydGlmaWNhdGVzL.WRwZ5sb2FkLlfFORlNlY5VyZVNlcnZl
cIJvb3RDQS5jZXIwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAPLs8bOhwwNPG
3Ivjl7adP++ORgvrfLb42tpCw9sa60Gp9S7bHFD2KLRaNfDs7FNwz2NFBkWytctXO7IlLCn1plUx
FVa89NcuGsJggna5rd30dHDr3XgNVdVB2kmCHXARdeXApaRyGiXk0kJwjSNzvnjG+Wbp7s/1/
bCe7hchgHJ6oCrnyRQFF1c1Ts5ghQCNzLngWWdfOY5V1+jQk87InDbEpLKVSrLXrWYJuWLykUR8HV
sh3U/AeRcbi73tejaPSQ5vqi012YCK89zFujWmSCIRPLhViR9Cpalza/spKaNfo4O4hxiat4YoMq
73rT+2sj3fswF4V1oopSoLbPvL9HLynQpLB2wB6fsWz7kmPEkbfx+GWmx10WAJA2TCSdPdUUAfzz
NAcPI6f3b1+svYr5UpS8KurXv9HuS/clEpa7FSb8QecC3OcWYY6NtuT72LnGJUQUjKu1DcGh
MoL6b1OPBYyjPXBEsol9vQzws4tYTkIGxYw2R79ntCM66ziTF+xAefjdHM/VYXBzk7fsAmgOJpJ
VkFwEx20mAzNr36fJkL596v7ma2hYxhE/tUB5PfThi6PUGblb+ce/zlcfVPOAPnUbGPRETPuÜlFB
/U6WoD5Jl698g6C3WLKDh0nxmfdSy35ylcgIVOBVizEzoKVYXonwKwydvn+thXE=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF Secure Server Root CA*

Issuer OU: *ANF CA Raiz*

Issuer O: *ANF Autoridad de Certificacion*

Issuer C: *ES*

Issuer SERIAL NUMBER: *G63287510*

Subject CN:	*ANF High Assurance Server CA*
Subject OU:	*ANF Autoridad intermedia tecnicos*
Subject O:	*ANF Autoridad de Certificacion*
Subject C:	*ES*
Subject SERIAL NUMBER:	*G63287510*
Valid from:	*Thu Sep 05 18:35:44 CEST 2019*
Valid to:	*Sun Sep 02 18:35:44 CEST 2029*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DD:A8:CB:E2:42:F5:FD:04:9F:26:7A:93:C5:2E:94:00:88:38:A6:35:96:FD:D3:B5:CA:77:F6:C3:6E:D1:D0:54:3F:C8:4E:39:60:01:66:F6:B4:35:33:8F:4F:CA:99:5A:95:FE:AE:40:D6:96:CB:9B:74:C5:12:DA:A0:00:B0:C8:BF:BC:D3:0E:92:20:F4:CF:F2:1C:E6:3A:83:24:13:B2:8E:71:BC:12:9C:33:21:4D:05:CF:8B:F1:00:C8:45:DE:ED:89:99:41:F0:35:0F:19:2B:6D:92:72:63:B2:9F:63:ED:A7:31:88:CC:E9:DB:1B:5B:18:BF:A4:95:76:1D:06:D5:D9:44:6A:AA:13:C4:FC:F9:F8:4C:71:DD:90:89:1A:F2:D3:19:52:6B:4E:8D:08:15:75:C7:30:D2:86:61:42:23:51:F3:6C:3D:0B:5F:5F:D4:6A:88:A5:E5:43:62:F6:92:85:92:8E:0F:80:CA:0D:00:57:DA:69:42:2F:29:94:78:8D:38:A1:69:55:33:B5:5F:18:75:68:03:1A:30:F4:25:B0:10:08:E0:02:B9:23:6A:D9:0E:94:FB:D5:8B:C1:36:C3:E0:47:B1:55:98:C7:A0:15:0A:FD:3C:57:95:EE:7A:71:A0:1F:11:BA:CF:99:2E:9C:4A:95:9E:F0:0D:4B:3D:B1:E7:AA:19:BC:8A:C2:24:F5:C3:7B:13:E1:DD:C8:B2:17:DE:33:CB:BA:28:5D:25:6C:4B:0F:3B:1E:4F:D4:E3:C6:CC:BC:9E:6C:B1:43:85:7E:07:20:21:FC:10:2E:B3:78:09:3C:94:8C:EF:2F:4B:67:67:EB:11:42:4E:06:ED:EC:20:6F:A0:D9:C2:35:96:84:0A:63:AC:F6:E6:30:F5:ED:28:AD:47:E8:9F:5B:7F:67:99:84:97:06:F7:D5:8E:8A:E8:2D:8C:0E:65:A2:18:03:69:70:67:91:59:D9:67:14:A6:F5:D1:B9:C6:AD:94:89:47:AA:5C:86:BD:5F:AB:CA:59:89:8B:3A:5B:5C:EC:06:AE:70:3C:B0:DE:3F:1B:ED:1C:33:3F:0F:A5:EB:E4:48:A7:29:23:D9:AB:20:CD:EF:68:A2:3D:E8:65:94:10:3E:F3:36:F6:B4:8E:73:76:5E:20:2F:C1:AE:0D:BF:CC:B1:27:49:60:7F:3E:E0:AB:58:0A:C8:6A:F7:7B:99:4B:D4:37:00:63:7B:B3:88:9D:19:C6:64:3F:88:DA:61:B4:37:C9:69:E2:E1:3B:85:2B:81:E4:A2:3F:46:70:8D:0D:CD:BE:5E:A0:9A:16:39:DC:98:20:A3:8D:72:8B:3F:9F:51:29:5F:6A:15:47:CD:02:03:01:00:01*
Authority Key Identifier	*9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37*
Subject Key Identifier	*94:BA:FA:EE:22:FA:32:1C:CB:05:77:B7:19:AF:12:F0:9A:6C:47:AB*
Extended Key Usage	*id_kp_clientAuth - id_kp_serverAuth*
CRL Distribution Points	*http://crl.anf.es/crl/ANFSecureServerRootCA-arl.crl* *http://www.anf.es/crl/ANFSecureServerRootCA-arl.crl*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.anf.es/es/documentos*
Authority Info Access	*http://ocsp.anf.es/spain/AV* *http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer*
Basic Constraints	*IsCA: true*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*8A:F5:5A:7E:98:53:66:24:CD:3E:4C:DC:EE:7F:7C:C5:91:46:0D:B7:81:BA:84:50:BA:05:3B:06:96:95:C1:74*

X509SubjectName

Subject CN:	*ANF High Assurance Server CA*
Subject OU:	*ANF Autoridad intermedia tecnicos*
Subject O:	*ANF Autoridad de Certificacion*

Subject C: *ES*

Subject SERIAL NUMBER: *G63287510*

X509SKI

X509 SK I *lLr67iL6MhzLBXe3Ga8S8JpsR6s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-03-17T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

6.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

6.7.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by ANF High Assurance Server CA*

Name *[es]* *Certificados cualificados emitidos por ANF High Assurance Server CA*

Service digital identities

X509SubjectName

Subject CN: *ANF High Assurance Server CA*

Subject OU: *ANF Autoridad intermedia tecnicos*

Subject O: *ANF Autoridad de Certificacion*

Subject C: *ES*

Subject SERIAL NUMBER: *G63287510*

X509SKI

X509 SK I *lLr67iL6MhzLBXe3Ga8S8JpsR6s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-11-25T01:00:00Z*

6.7.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

6.8 - Service (granted): Qualified timestamps issued by ANF High Assurance Server CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by ANF High Assurance Server CA*

Name *[es]* *Sellos de tiempo cualificados emitidos por ANF High Assurance Server CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *99659964253702882*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHhDCCBWygAwIBAgIIAWIQNZ+riuIwDQYJKoZIhvcNAQELBQAwgYQxEjAQBgNVBAUTCUc2MzI4
NzUxMDELMAkGA1UEBhMCRVMxJzAlBgNVBAoTHkFORiBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lv
bjEUMBIGA1UECxMLQU5GIENBIFJhaXoxIjAgBgNVBAMTGUFORiBTZWN1cmUgI2VydmVyIFJvb3Qg
Q0EwHhcNMTkwOTA1MTYzNTQ0WhcNMjkwOTAyMTY2NTQ0WjCBnTESMBAGA1UEBRMJRzYzMjg3NTEw
MQswCQYDVQQGEwJFUzEnMCUGA1UEChMeQU5GIEF1dG9yaWRhZCBlZSBDZXJ0aWZpY2FjaW9uMSow
KAYDVQQLEyFBTkYgQXV0b3JpZGFkIGludGVybWVkaWEgdGVjbmljb3MxJTAjBgNVBAMTHEFORiBI
aWdoIEFoc3VyYW5jZSBTZXJ2ZXIgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDd
qMviQxX9BI8mepPFLpQAiDimNZb907XKd/bDbtHQVD/TjlgAWb2tDUzj0/KmVqV/q5A1pbLm3TF
EtgzALDIv7zTDplg9M/yHOY6tyQTso5xvBKeMyFNBc+L8QDIRd7tiZIB8DU/PGStknJjsp9j7acx
iMzp2xtbGL+kIXydBtXZRGqqE8T8+thMcd2QiRry0xISa06NCBV1xzDShmFC11HzbD0LX1/Uaoil
5UNi9pKFko4PgMoNAFfaaUlyKZR4jTihaV1zVS8YdWgDGjD0IbAQCOACuSNq2Q6U+9WLwTbD4Eex
VZHoBUK/TxXIe56caAIEbrPmN6cNpWe8A1LPbHnqhm8isIk9cN7E+HdyLIX3jPLuibdJWxLDzse
T9Tjxsy8nmyxQ4V+ByAh/BAus3gJPJSM7y9LZ2frEUJOBu3sIG+g2e11loQKY6z25jD17SitR+if
W39nmYSXBvfVjoroLYwOZaIYA2lwZSFZ2WcUpvXRucatIIHqIyGvV+rylmJizpbXOwGrnA8sN4/
G+0cMz8PpevkSKcpl9mrIM3vaKI96GWUED7zNva0jnN2XiAvwa4Nv8yxJ0lgfz7gq1gKyGr3e5IL
1DcAY3uzJf0ZxmQ/iNpbtD0zeLbOMUzgeSiP0ZwjQ3Nvl6gmbY53Jggo4Iyz+fU/SIfabVHzQID
AQABo4IB3TCCAdkwHwYDVR0jBBgwFoAUnF/QbGOjX5PKk5gIrYyHpSxcwTcwHQYDVR0OBBYEFJS6
+u4i+jIcywV3txmvEvCabEcrMA4GA1UdDwEB/wQEAwIBhjAnBgNVHSUEIDAeBggrBgEFBQcDAQYI
KwYBBQUHAwIGCCsGAQUFBwMDMH8GA1UdHwR4MHYwOaA3oDWGM2h0dHA6Ly9jcmwuYW5mLmVzL2Ny
bC9BTkZTZWN1cmVTZXJ2ZXJSb290OI6YXJsLmNvbDA5oDegNYYzaHR0cDovL3d5dy5bbmYuZXMv
Y3JsL0FORlNlY3VyZVNlcnZlclVb3RDQS1hcmwuY3JsMEAGA1UdIAQ5MDcwNQYEVR0gADAtMCsG
CCsGAQUFBwIBFh9odHRwOi8vd3d3LmFuZi5lcy9lcy9kb2N1bWVudG9zMIGJBggrBgEFBQcBAQR9
MHswJwYIKwYBBQUHMAGGG2h0dHA6Ly9vY3Nwl.mFuZi5lcy9zcGFpb9BVjBQBggrBgEFBQcwAoZE
aHR0cDovL3d3dy5bbmYuZXMvZXMvY2VydGlmaWNhdGVzL WRvdZ5sb2FkL0FORlNlY3VyZVNlcnZl
clVb3RDQS5jZX1wDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAPLs8bOhwwNPG
3fvjl7adP++ORgvrfLb42tpCw9sa60Gp9S7bHFD2KLRaNtDs7FNwz2NFBkWytctXO7IlLCn1plUx
FVa89tNeuGsJlggna5rd30dHDr3XgNVdVB2kmCHXARdgXApaRyGiXk0kjwjSNizvijG+Wbp7s/1/
bCef7hchgHJoCmyRQEF1c1b5qbtQCSr1ngWWdtOY5V/+jQd87JnDbEpLKVSrLXrWYJuWLykUR8HV
sh3U/AeRcbi73tejaPSQ5vqi012YCK89zFujWmSClRPLbViR9Cpalza/spKaNfo4O4hxiat4YoMq
73rT+2sj3fswF4V1oopSoLbPvL9HLynQpLB2wB6f8Wz7kmPEkbfx+GWmx10WAJA2TCSdPdUUAfzz
NAcPI6f3b1+svYr5UpS8KurXiv9HuS/clEpa7FSb8QecC3OeW8YYQ6Nu/T2LnGJUQUjKu1DcGh
MoL6b1OPBYyjPXBEso9wQzws4YTkKcxYw2R79otC3M6ziTF+xAeljdJhM/VVXBxrk7fsAmgOIpJ
VkFwfx20mAzNz36fJkL596v7ma2hYxhE/tU/B5PfTho6PUGbIb+ce/zlefVPOAPnUbGPRETPuUlF/B
/U6WoD5JI698g6C3WLKDh0nxmfdSy35ylcgIVOBVizEzoKVYXonwKwydvn+thXE=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ANF Secure Server Root CA*
Issuer OU:	*ANF CA Raiz*
Issuer O:	*ANF Autoridad de Certificacion*
Issuer C:	*ES*
Issuer SERIAL NUMBER:	*G63287510*
Subject CN:	*ANF High Assurance Server CA*
Subject OU:	*ANF Autoridad intermedia tecnicos*
Subject O:	*ANF Autoridad de Certificacion*
Subject C:	*ES*
Subject SERIAL NUMBER:	*G63287510*
Valid from:	*Thu Sep 05 18:35:44 CEST 2019*
Valid to:	*Sun Sep 02 18:35:44 CEST 2029*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DD:A8:CB:E2:42:F5:FD:04:9F:26:7A:93:C5:2E:94:00:88:38:A6:35:96:FD:D3:B5:CA:77:F6:C3:6E:D1:D0:54:3F:C8:4E:39:60:01:66:F6:B4:35:33:8F:4F:CA:99:5A:95:FE:AE:40:D6:96:CB:9B:74:C5:12:DA:A0:00:B0:C8:BF:BC:D3:0E:92:20:F4:CF:F2:1C:E6:3A:83:24:13:B2:8E:71:BC:12:9C:33:21:4D:05:CF:8B:F1:00:C8:45:DE:ED:89:99:41:F0:35:0F:19:2B:6D:92:72:63:B2:9F:63:ED:A7:31:88:CC:E9:DB:1B:5B:18:BF:A4:95:76:1D:06:D5:D9:44:6A:AA:13:C4:FC:F9:F8:4C:71:DD:90:89:1A:F2:D3:19:52:6B:4E:8D:08:15:75:C7:30:D2:86:61:42:23:51:F3:6C:3D:0B:5F:5F:D4:6A:88:A5:E5:43:62:F6:92:85:92:8E:0F:80:CA:0D:00:57:DA:69:42:2F:29:94:78:8D:38:A1:69:55:33:B5:5F:18:75:68:03:1A:30:F4:25:B0:10:08:E0:02:B9:23:6A:D9:0E:94:FB:D5:8B:C1:36:C3:E0:47:B1:55:98:C7:A0:15:0A:FD:3C:57:95:EE:7A:71:A0:1F:11:BA:CF:99:2E:9C:4A:95:9E:F0:0D:4B:3D:B1:E7:AA:19:BC:8A:C2:24:F5:C3:7B:13:E1:DD:C8:B2:17:DE:33:CB:BA:28:5D:25:6C:4B:0F:3B:1E:4F:D4:E3:C6:CC:BC:9E:6C:B1:43:85:7E:07:20:21:FC:10:2E:B3:78:09:3C:94:8C:EF:2F:4B:67:67:EB:11:42:4E:06:ED:EC:20:6F:A0:D9:C2:35:96:84:0A:63:AC:F6:E6:30:F5:ED:28:AD:47:E8:9F:5B:7F:67:99:84:97:06:F7:D5:8E:8A:E8:2D:8C:0E:65:A2:18:03:69:70:67:91:59:D9:67:14:A6:F5:D1:B9:C6:AD:94:89:47:AA:5C:86:BD:5F:AB:CA:59:89:8B:3A:5B:5C:EC:06:AE:70:3C:B0:DE:3F:1B:ED:1C:33:3F:0F:A5:EB:E4:48:A7:29:23:D9:AB:20:CD:EF:68:A2:3D:E8:65:94:10:3E:F3:36:F6:B4:8E:73:76:5E:20:2F:C1:AE:0D:BF:CC:B1:27:49:60:7F:3E:E0:AB:58:0A:C8:6A:F7:7B:99:4B:D4:37:00:63:7B:B3:88:9D:19:C6:64:3F:88:DA:61:B4:37:C9:69:E2:E1:3B:85:2B:81:E4:A2:3F:46:70:8D:0D:CD:BE:5E:A0:9A:16:39:DC:98:20:A3:8D:72:8B:3F:9F:51:29:5F:6A:15:47:CD:02:03:01:00:01*
Authority Key Identifier	*9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37*
Subject Key Identifier	*94:BA:FA:EE:22:FA:32:1C:CB:05:77:B7:19:AF:12:F0:9A:6C:47:AB*
Extended Key Usage	*id_kp_clientAuth - id_kp_serverAuth*
CRL Distribution Points	*http://crl.anf.es/crl/ANFSecureServerRootCA-arl.crl* *http://www.anf.es/crl/ANFSecureServerRootCA-arl.crl*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.anf.es/es/documentos*
Authority Info Access	*http://ocsp.anf.es/spain/AV* *http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer*
Basic Constraints	*IsCA: true*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *8A:F5:5A:7E:98:53:66:24:CD:3E:4C:DC:EE:7F:7C:C5:91:46:0D:B7:81:BA:84:50:BA:05:3B:06:96:95:C1:74*

X509SubjectName

Subject CN: *ANF High Assurance Server CA*

Subject OU: *ANF Autoridad intermedia tecnicos*

Subject O: *ANF Autoridad de Certificacion*

Subject C: *ES*

Subject SERIAL NUMBER: *G63287510*

X509SKI

X509 SK I *lLr67iL6MhzLBXe3Ga8S8JpsR6s=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2019-11-25T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

6.9 - Service (granted): Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AC Servicio de validación

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

Service type description *[en]* *undefined.*

[es] *undefined.*

Service Name

Name *[en]* *Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AC Servicio de validación*

Name *[es]* *Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados por ANF AC Servicio de validación*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *996911385882141775209901911*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHrzCCBeegAwIBAgIMAzigMoR3cx2try9XMA0GCSqGSIb3DQEBCwUAMIIBITELMAkGA1UEBhMC
RVMxEjAQBgNVBAgMCUlhcmNlbG9uYTFYMFYGA1UEBwxPQmFyY2Vsb25hIChzZWUgY3VycmVudCBh
ZGRyZXNzIGF0IGh0dHA6Ly93d3cuYW5mLnVzL2VzL2FkZHJlc3MuZGhyZWNjaW9uLmh0bWwgKTEn
MCUGA1UECgwcQU5GIEF1dG9yaWRhZCBkZSBlZXJ0aWZpY2FjaW9uMS4wLAYDVQQLDCVBTkYgQXV0
b3JpZGFkIEludGVvbWVkaWEgZGUgSWRlbnRpZGFkMRowGAYJKoZIhvcNAQkBFgtpbmZvQGFuZi5l
czESMBAGA1UEBRMJRzYzMjg3NTEwMRswGQYDVQQDDBJBTkYgQXNzdXJlZCBJRCBDQTEwHhcNMjAx
MjAzMTYwMDU3WhcNMjIxMjAzMTYwMDU3WjCB9zELMAkGA1UEBhMCRVMxEjAQBgNVBAgMCUNhdGFs
dc0xYTESMBAGA1UEBxMJQmFyY2Vsb25hMScwJQYDVQQKEx5BTkYgQXV0b3JpZGFkIGRlIENlcnRp
ZmlqYWNpb24xNTAzBgNVBAsTLENlcnRpZmlqYWRvIEN1YWxpZmlqYWRvIGRlIFNlbGxvIEVsZWN0
cm9uaWNvMR0wGwYJKoZIhvcNAQkBFg5zb3BvcnRlQGFuZi5lczEnMCUGA1UEAwweQUSGIEFDIFNl
cnZpY2lvIGRlIHZhbGlkYWNpw7NuMRgwFgYDVQRhEw9WQVRFUy1HNjMyODc1MTAwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9CNlOoLuMEAwHEZtI2B+j4Z8qSgNkzm92sd59lM35EcVG
6TMsEMW3zzuI4R3EWzf90kXXVy2Bs9tIwymw8dtUqvO7mTQsgt0khnKqMzj/yGZv1KCQRdJI9uDg
q0Q+Ga1Ho90iFC/UnR8FbXmOI3n4gAUP40J0ETFLFiKA+4JoL6uCaBJOymX2gHLFtI8HDr0xO77X
BkSLT3TMmYyKnuY7XqnEYQ1FTMtDB6aS6F91wSPPIVsLTLB/LLRKVD+3rlELkOiMy0Kq/Pn7oIaI
sXTqtkJuNnQS3FM+AgEG41Vu4FXsUfsE5z08E83xY6dM5xQrmYRcIcr/zpPtGeC2INKvAgMBAAGj
ggIcMIICWDAfBgNVHSMEGDAWgBQ1Uz3mKRy/i9lKDJ4rAIVH0cZPPTAdBgNVHQ4EFgQLd/hl/Poi
3FH9iXPkkEm1swBJgswGQYDVR0RBBIwEIEOc29wb3J0ZUBhbmYuZXMwDgYDVR0PAQH/BAQDAgXg
MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDBFBgNVHR8EPjA8MDqgOKA2hjRodHRwczov
L3d3dy5hbmYuZXMvY3JsL0FORI9Bc3N1cmVkX0lEX0NBMV9TSEEyNTYuY3JsMFEGA1UdIARKMEgw
OwYMKwYBBAGBjxwZAQEBMCswKQYIKwYBBQUHAgEWHWhtdHRzOi8vd3d1LmFuZ5Icy9kb2NlbWVu
dG9zMAkGBwQAi+xAAQEwgY4GCCsGAQUFBwEBBIGBMH8wJwYIKwYBBQUHMAGGG2h0dHA6Ly9vY3Nw
LmFuZi5lcy9zcGFpbi9BVjBUBggrBgEFBQcwAoZIaHR0cDovL3d3dy5hbmYuZXMvZXMvY2VydGlm
aWNhdGVzX2Rvd25sb2FkL0FORI9Bc3N1cmVkX0lEX0NBMV9TSEEyNTYuY2VyMAwGA1UdEwEB/wQC
MAAwbAYIKwYBBQUHAQMEYDBeMAoGCCsGAQUFBwsCMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wJAYG
BACORgEFMBowGBYSaHR0cHM6Ly9hbmYuZXMvZW4vEwJlbjATBgYEAI5GAQYwCQYHBACORgEGAjAI
BgkrBgEEAYGPHBMEGAwWNTAyNDQ5MzQwLTQ3NDM3MzQ4MjQ0MDANBgkqhkiG9w0BAQsFAAOCAgEA
gxqtVj3kLh3sA9u3b9SPbizgkj1LiFfxGRIFKX9eOTeZoNzXt2g+HgNQdvOQ75m0VMbKKyqqvs3r
fSym8rr90+XemcvfthE2ladlKeeGH0fsbCfYw8h2De1hzoNPG+ne/WqarcYAdHfGZMr3atzn1OBY
vj/gtSiq1ysWVgCY+vtzU/AwrPSJgHEF+T2/+ithj1CJAXS8KBYin2cs6RmaZGh2ZnJKQb4fH4
4OAmeGPyX1Ro3AHdV1wxGN4v0MuZ0NwLPNm0yGnSyyVwkiqftv3XjpgMn/5Nu/K481JuicLXx5DR
RPBPPOHKobYasdZFbkCUZRUnBug+7MccPo5IeYgMvlEOThmfl+UUr/z2hxnoudGYmLLbH8cn+Kcy
UrXHqvTsJiY4mRmQy2kMoR1datLYcuVmOsu8VHi49Id6ruFbAMmHU71K/BsvUTm260ck5Kt9HB
x7pt29hIDpsQq8Am1+HIDM3zMfw58LRXiDocFoNHu0LLgTbfcSc5b60pHP354PKpUw5czhAOBjW
wE0cNZqtCHJq+++zTgaqvyyewOQ/BITxSQZUTjzbQ95AZfc0dR9TBwPxvUCtv8bWelO9c/oVhEsE
PMFK/b9l8Qu3BuORqKo0SaA1nT10RJK5wCoTHqdGmQazJf1lVfFfphGMkhjqcaI50AN3jmD6nfI=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF Assured ID CA1*

Issuer SERIAL NUMBER: *G63287510*

Issuer E: *info@anf.es*

Issuer OU: *ANF Autoridad Intermedia de Identidad*

Issuer O: *ANF Autoridad de Certificacion*

Issuer L: *Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*

Issuer ST: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-G63287510*

Subject CN: *ANF AC Servicio de validación*

Subject E: *soporte@anf.es*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona*

Subject ST: *Cataluña*

Subject C: *ES*

Valid from:	*Thu Dec 03 17:00:57 CET 2020*
Valid to:	*Sat Dec 03 17:00:57 CET 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BD:08:D9:4E:A0:BB:8C:10:0C:09:11:9B:5F:D8:1F:A3:E3:64:6A:4A:03:64:CE:7F:76:B1:DE:7D:94:CD:F9:11:E5:46:E9:33:2C:10:C5:B7:CF:3B:89:E1:1D:C8:11:6C:C8:F7:49:17:5D:5C:B6:06:CF:6D:23:0C:A6:C3:C7:6D:52:AF:CE:EE:6D:50:AA:0D:24:86:72:AA:33:38:FF:C8:66:6F:D4:A0:90:45:D2:48:F6:E0:E0:AB:44:3E:19:AD:47:A3:DD:22:14:2F:D4:9D:1F:05:6D:79:8E:23:79:F8:80:05:0F:E3:42:74:11:31:4B:16:22:80:FB:82:68:2F:AB:82:68:12:4E:CA:65:F6:80:72:C5:B4:8F:07:0E:BD:31:3B:BE:D7:06:44:8B:4F:74:CC:99:8C:8A:9E:E6:3B:5E:A9:C4:61:0D:45:4C:C7:C3:07:A6:92:E8:5F:75:C1:23:CF:95:5B:0B:4C:B0:7F:2C:B4:4A:54:3F:B7:AD:F1:0B:90:E8:8C:CB:42:AA:FC:F9:FB:A0:86:88:B1:74:EA:8A:42:6E:36:74:12:DC:53:3E:02:01:06:E3:55:6E:E0:55:EC:51:FB:04:E7:3D:3C:13:CD:F1:63:A7:4C:E7:14:2B:99:84:5C:21:CA:FF:CE:93:ED:19:E0:B6:20:D2:AF:02:03:01:00:01*
Authority Key Identifier	*35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*
Subject Key Identifier	*77:F8:48:FC:FA:22:DC:51:FD:89:73:E4:90:49:B5:B3:00:7F:26:0B*
Subject Alternative Name	*soporte@anf.es*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18332.25.1.1.1* *CPS pointer: https://www.anf.es/documentos* *Policy OID: 0.4.0.194112.1.1*
Authority Info Access	*http://ocsp.anf.es/spain/AV* *http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer*
Basic Constraints	*IsCA: false*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*8D:25:C0:1A:24:CB:58:33:E4:97:46:90:D1:11:36:0A:B1:2A:F0:72:21:FD:8C:0C:7D:41:22:D9:12:54:65:C7*

X509SubjectName

Subject 2.5.4.97:	*VATES-G63287510*
Subject CN:	*ANF AC Servicio de validación*
Subject E:	*soporte@anf.es*
Subject OU:	*Certificado Cualificado de Sello Electronico*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona*

Subject ST: *Cataluña*

Subject C: *ES*

X509SKI

X509 SK I *d/hI/Poi3FH9iXPkkEm1swB/Jgs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2021-01-26T01:00:00Z*

6.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.10 - Service (granted): Qualified electronic registered delivery service ANF AC

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description [en] *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name [en] *Qualified electronic registered delivery service ANF AC*

Name [es] *Servicio cualificado de entrega electrónica certificada de ANF AC*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *99618787124707912922716429 7*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIH/zCCBeegAwIBAgIMAzgG/LXjpnc5G3qJMA0GCSqGSIb3DQEBCwUAMIIBITELMAkGA1UEBhMC
RVMxEjAQBgNVBAgMCUlhcmNlbG9wYTFYMFYGA1UEBwxPQmFyY2Vsb25hNChzZWUgY3VycmVuaCBh
ZGRyZXNzIGF0IGhldHA6Ly93d3cuYW5mLmVzL2VzLFRzHJlc3MtZGlyZWNjaW9uLmhlbWwgKTEn
MCUGA1UECgweQU5GIEF1dG9yaWRhZCBlZSBDZXJ0aWZpY2FjaW9uMS4wLAYDVQQLDCVBTkYgQXV0
b3JpZGFkIEludGVvbVkaWEgZGUgSWRlbnRpZGFkMRowGAYJKoZIhvcNAQkBFgtpbmZvQGFuZi5l
czESMBAGA1UEBRMJRzYzNDIg3NTEwMRswGQYDVQQDDBJBTkYgQXNzdXJlZCBJRCBDQTEwIhcNMjAx
MjAyMTI1MjI2WhcNMjIxMjAyMTI1MjI2WjCB9zELMAkGA1UEBhMCRVMxEjAQBgNVBAgMCUNhdGFs
dcOxYTESMBAGA1UEBxMJQmFyY2Vsb25hMScwJQYDVQQKEx5BTkYgQXV0b3JpZGFkIGRlIENlcnRp
ZmljYWNpb24xNTAzBgNVBAsTLENlcnRpZmljYWRvIEN1YWxpZmljYWRvIGRlIFNlbGxvIEVsZWN0
cm9uaWNvMR0wGwYJKoZIhvcNAQkBFg5zb3BvcnR1QGFuZi5lczEnMCUGA1UEAxMcU2lnbiB0byBT
aWdulERlbGl2ZXI5IFNlcnZpY2VzMRgwFgYDVQRhFw9WQVRFUy1HNjMyODc1MTAwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDIzKdoZFj4nIsJPpYc3EAxORcW1zf6OE+neI29RChl+Cax
M8kFkl8SHJZKPhqY4+JGi9v5ZdP6Btg7aMlWhRtPa2MS2RrmOkqNMYridaUizTYTR5k43mhvIW7lw
vorkTv/VXbY6RYKFJg9yQbD5nIjKBJhdnwCiDnYy16pMjU4iXyccHFU2UM6gIt1SblOSkSwF/9D3
uYSkqnqjbJPk5Yx6qrcYLAH0vYCBZrFZcCLK/VmR1KlU11aVfYa++wqpF4tRYMKu7k+krNQKA19
9ahzAh0+AR3SH2DJ7SvJbO8ClcCRYgRRjmrRhY0X87K2pxNcAp9r/PqgeS+7Zs5YJRlvAgMBAAGj
ggJcMIICWDAfBgNVHSMEGDAWgBQ1Li3mKRy/i9lKf34r4JVH0cZPPTAdBgNVHQ4EFgQUebLudB3q
/eytq7utI/KmzdRLXIIwGQYDVR0RBBIwEIEOc29wb3J0ZUBhbmYuZXMwDgYDVR0PAQH/BAQDAgXg
MB0GA1UdJQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDBFBgNVHR8EPjA8MDugOKA2hjRodHRwczov
L3d3dy5hbmYuZXMvY3JsL0FORI9Bc3N1cmVkX0lEX0NBMV9TSEEyNTYuY3JsMFEGA1UdIARKMEgw
OwYMKwYBBAGBjxwZAQEBMCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vd3d3LmFuZi5lcy9kb2N1bWVu
dG9zMAkGBwQAi+xAAQEwgY4GCCsGAQUFBwEBIGBMH8wJwYIKwYBBQUHMAGGG2h0dHA6Ly9vY3Nw
LmFuZi5lcy9zcGFpbi9BYiBUBggrBgEFBQcwAoZlaHR0cDovL3d3dy5hbmYuZXMvZXMvY2VvdGlm
aWNhdGVzX2Rvd25sb2FkL0FORI9Bc3N1cmVkX0lEX0NBMV9TSEEyNTYuY2VvMAwGA1UdEwEB/wQC
MAAwbAYIKwYBBQUHAQMEYDBcMAoGCCsGAQUFBwsCMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wJAYG
BACORgEFMBowGBYSaHR0cHM6Ly9hbmYuZXMvZW4vEwJlbjATBgYEAI5GAQYwCQYHBACORgEGAjAI
BgkrBgEEAYGPHBMEGAwWNTAyMzE1Nzg3L TQ3NDM3MzQ4MjQ0MDANBgkqhkiG9w0BAQsFAAOCAgEA
CAO1zTwyI8+B27Vck9YVB+KOzKuREKH1xD5NeY0MLnr82mduaxV79hbfwqUGMVT7qSLM9N4QTyu
PMFVLpFxGwcluQ/LVjyWPbHnMiK/+aWB3I6uA2vIAGNOHNL3bRvGl1PvJ8E2Q/SFdEDSKYW8fFR
b8In2V lcGzGNSWY77RG7i+gXIXpO9aiuJ0dcV7Atsy/527xjJ00ktsZ2vmvnRMJ5OjUkR6+UyBBb
VTlq4iGtcG4q9HMJmnN+tAWVHV8QF1outIATuMbpHyywHjbdjP/y+GSORvpn+7k4MwVxaQdXT8l
nspfVPsP35WbMc31SCRY2IVpc6JIuzHCmWGeRvdt15L nrTmqmkErwYrpIXLjZiULYvm9mm
/kl/JTCcVPeegKYcAn3rySwbFZxoduQbg9I3W+kQaTSZXERX+q6H+xkE6fMpnv2nDRBadFIbcsV
qLvf98GB7muWSoIQq7CnTyZjeUuoPkIaJLJFJg6QbEVrWGhf8dX22zspReQFRmZPM/MjMpcryRv
KvgBJs/hYpleCT0/87pCQXfo0U7wrqTBH2tCRnQJ4uRtK8Px3KXyZq5BTVxlmyTMPlAJDl9J5tl
DhfWkNYieFHoDx0cPtDmyTDoya2M9MBqYv+bmo4otxWMs4Ojd0sdRxYwWNAIKc4CSD0ngXqSE8k=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF Assured ID CA1*

Issuer SERIAL NUMBER: *G63287510*

Issuer E: *info@anf.es*

Issuer OU: *ANF Autoridad Intermedia de Identidad*

Issuer O: *ANF Autoridad de Certificacion*

Issuer L: *Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*

Issuer ST: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-G63287510*

Subject CN: *Sign to Sign Delivery Services*

Subject E: *soporte@anf.es*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona*

Subject ST: *Cataluña*

Subject C: *ES*

Valid from: *Wed Dec 02 13:52:56 CET 2020*

Valid to: *Fri Dec 02 13:52:56 CET 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:CC:A7:68:64:58:F8:9C:8B:09:3E:96:1C:DC:40:31:39:17:16:D7:37:FA:38:4F:A7:78:8D:BD:44:28:48:F8:26:B1:33:C9:05:90:8F:12:1D:92:8F:86:A6:38:F8:91:A2:F6:FE:59:74:FE:81:B6:0E:DA:32:55:A1:46:B3:DA:D8:C4:B6:46:B9:8E:92:A3:4C:62:B8:9D:69:48:B3:4D:84:D1:E6:4E:37:9A:1B:E5:5B:B2:30:BE:8A:E4:4E:FF:D5:5E:16:3A:45:82:85:26:0F:72:42:10:F9:9C:88:CA:04:98:5D:B7:00:A2:0E:76:32:D7:AA:4C:8D:4E:22:5F:27:1C:1C:55:36:50:CE:A0:22:27:D2:6E:53:92:91:2C:05:FF:D0:F7:B9:84:A4:AA:77:23:6C:93:E4:E5:8C:7A:AA:B7:95:2C:01:F4:BD:80:81:66:B1:59:78:22:CA:FC:95:66:45:42:94:53:5D:3A:55:F6:1A:FB:EC:2E:A4:52:38:45:83:0A:BB:B9:3E:92:B3:4E:28:0D:7D:F5:A8:73:02:1D:3E:01:1D:D2:1F:60:C9:ED:2B:C9.6C:EF:02:95:C0:91:62:04:51:8E.6A:D1:85:8D:17:F3:B2:B6:A7:13:5E:02:9F:6B:FC:FA:A0:79:2F:BB:66:CE:58:25:19:6F:02:03:01:00:01

Authority Key Identifier

35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D

Subject Key Identifier

79:B2:EE:74:1D:EA:FD:EC:AD:AB:BB:AD:23:F2:A6:CD:D4:4B:5D:F2

Subject Alternative Name

soporte@anf.es

Extended Key Usage

id_kp_clientAuth

CRL Distribution Points

https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl

Certificate Policies

Policy OID: 1.3.6.1.4.1.18332.25.1.1.1

CPS pointer: https://www.anf.es/documentos

Policy OID: 0.4.0.194112.1.1

Authority Info Access

http://ocsp.anf.es/spain/AV

http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer

Basic Constraints

IsCA: false

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

Key Usage:

digitalSignature - nonRepudiation - keyEncipherment

Thumbprint algorithm:

SHA-256

Thumbprint:

20:94:FB:22:EC:CD:E5:50:9C:B8:87:D5:B8:34:2D:84:0C:75:D0:5E:46:1D:B7:82:00:14:0D:18:22:B8:3C:94

X509SubjectName

Subject 2.5.4.97:

VATES-G63287510

Subject CN:

Sign to Sign Delivery Services

Subject E:

soporte@anf.es

Subject OU:

Certificado Cualificado de Sello Electronico

Subject O:

ANF Autoridad de Certificacion

Subject L:

Barcelona

Subject ST:

Cataluña

Subject C:

ES

X509SKI

X509 SK I *ebLudB3q/eytq7utI/KmzdRLXfI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-03-17T01:00:00Z*

6.11 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals by ANF AC

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service type description *[en]* *A preservation service for qualified electronic signatures.*

[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name *[en]* *Qualified preservation service for qualified electronic signatures and qualified electronic seals by ANF AC*

Name *[es]* *Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados de ANF AC*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *99618718687293327260772135 19*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJATCCBemgAwIBAgIMIDBEbBrcm8mXVktPMA0GCSqGSIb3DQEBCwUAMIIBITELMAkGA1UEBhMC
RVMxEjAQBgNVBAgMCUlhcmNlbG9uYTFYMFYGA1UEBwxPQmFyY2Vsb25hIChzZWUgY3VycmVudCBh
ZGRyZXNzIGF0IGh0dHA6Ly93d3cuYW5mLmVzL2VzL2FkZHJlc3MzZGlyZWNjaW9uLmh0bWwgKTEn
MCUGA1UECgwcQU5GIEFtdG9yaWRhZCBkZSBDZXI0aWZpY2FjaW9uMS4wLAYDVQQLDCVBTkYgQXV0
b3JpZGFkIHJhdGVybWVkaWEgZGUgSWRlbmRpZGFkMRowGAYJKoZIhvcNAQkBFgtpbmZvQGFuZi5l
czESMBAGA1UEBRMJRzYzMjg3NTEwMRswGQYDVQQDDBJBTkYgQXNzdXJlZCBJRCBDQTEwHhcNMjAx
MjAzMTAwMTAwWhcNMjIxMjAzMTAwMTAwWjCB+TELMAkGA1UEBhMCRVMxEjAQBgNVBAgMCUNhdGFs
deOxYTESMBAGA1UEBxMJQmFyY2Vsb25hMScwJQYDVQQKExSBTkYgQXV0b3JpZGFkIGRlIFNlcnRp
ZmljYWNpb24xNTAzBgNVBAsTLENlcnRpZmljYWRvIENlYWxpZmljYWRvIGRlIFNlbGxvIEVsZWN0
cm9uaWNvMR0wGwYJKoZIhvcNAQkBFg5zb3BvcnR1QGFuZi5lczEpMCcGA1UEAwwgQU5GIEFDIFNl
cnZpY2lvIGRlIGNvbnNlcnZhY2nDs24xGDAWBgNVBGETD1ZBVEVTLUc2Mzl4NzUxMDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKU/+4DXmdCAdShiF3z6xUNp52ngZsW3h7NR94+i2GiSQ
lSv2lGvPj/sTQdsNPQqdOhaqtJNMLoEw9/7U/j08jHoC7nLZTq5NlNaC2JVAHFEcz3anpYUSMdE8t
Z9ddFrCvGyAinwi4v7lm59HB6ud5pdmtuBQHYsWWtGC5GCs+U3ufOaNVCopWdlkumiklcA7Jjyuo
K0xSQhjDaW8VrKfWTr67ma4/83ioDjg625OajzY517ecOz6mOI/4wmeLbJ2abXKsLDmDkB+BBor
rVc3TD+fPcsw/ZTzGjhyTcW+nt5VEM7lI4+5EIn9+q9tgSsDx0vrCFYV3dFGlWXB1Pdj5V8CAwEA
AnOCAIwwggIYMBBGA1UdIwQYMBaAFDUuLsYpHL+L2UjnbnvgIU8ck89MB0GA1UdDgQWBBQRXouL
YiPrc9GVC8b4Be6j+xaSUzAZBgNVHREEEjAQgQ5zb3BvcnRlQGFuZi5lczAOBgNVHQ8BAf8EBAMC
BcAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEUGA1UdHwQ+MDwwOqA4oDaGNGh0dHBz
Oi8vd3d3LmFuZi5lcy9jcmwvQU5GX0Fzc3VyZWRlSUR1Q0ExX1N1QT1lNi5jcmwwUQYDVR0gBEow
SDA7BgwrBgEEAYGPHBkBAQEwKzApBggrBgEFBQcCARYdaHR0cHM6Ly93d3cuYW5mLmVzL2RvY3Vt
ZW50b3hwCQYHBACL7EABATCBjgYIKwYBBQUHAQEEgYEwfzAnBggrBgEFBQcwAYYbaHR0cDovL29j
c3AuYW5mLmVzL3NwYWluL0FWMFQGCCsGAQUFBzAChkhodHRwOi8vd3d3LmFuZi5lcy9lcy9jZXJ0
aWZpY2F0ZXNlZG93bmxvYWQvQU5GX0Fzc3VyZWRlSUR1Q0ExX1N1QT11Ni5jZXIwDAYDVR0TAQH/
BAIwADBsBggrBgEFBQcBAwRgMF4wCgYIKwYBBQUHCwIwCAYGBACORgEBMAsGiBgQAjkYBAwIBDzAk
BgYEAI5GAQI/wGjAYFhJodHRwczovL2FuZi5lcy9lbs8TAmVuMBMGBgQAjkYBBjAJBgcEAI5GAQYC
MCUGCSsGAQQBgY8cEwQYDBY0OTkzNjIwMTctNDc0MzczNDgyNDQwMA0GCSqGSIb3DQEBCwUAA4IC
AQANukfFUrNb2IvgG+NSi8OtxReGHA/Ib4a7c7aR9Hsb8XvGVFxvE/qIjvVu0DlbzIjYCpdlcwTP
+chZm0659xrLtxMJKv99R5LoQIw/e8NXeMym75IxZY0bcOFzFw9Msq3Va4REWGzrq0GwmeHIvBO7
XysjVxzbvNDzfxUhDnH8V1zqtk/5iymmkZ2tp0OXIAVmaPoDPa5WRE51JTJSi0ImAGzENieuNi5
ff2fhHHb412wHUdXKFx3QTIW1Q1DHkMBkpMv+B0ZLRYYSsy9XnyksdAsA2U/IhjeB88UWdImM2e6
D4Q5tzXvASo5swSzQdz+KQnD7ZnARJ78hZZdupbNMpyiJRMJGlNlAGCSUDYGPa6IrIqzsB0HQ81Q
mBK+eUTxHPZWq3hnNtJxZX+KxtEMNL44ZAnqwdJ66VIxLYxjrvIUtH6J1hH5GqHVeBvzaK6MwO
WIL/t09poIL7YcV4K2TrMfiQYckK41cdUsQpA+zEioJSCXuUv9sd2XUpwDUBS+9bTKyXg7art11ck
K7tmgMdadF674U34AptVwLVELbvLz8La4Ipd7DUYR5lfOkBu2HMczs2OyLZZOiE08Qxd1J1oXe5C
o2xnnA91ow/M5nnoJ30G1LB5/i9qFIRdIcFbDN03tzFBUSvm7+oYXc1pa0jJVFpPzKAl46W/qXUc
NQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF Assured ID CA1*

Issuer SERIAL NUMBER:	*G63287510*
Issuer E:	*info@anf.es*
Issuer OU:	*ANF Autoridad Intermedia de Identidad*
Issuer O:	*ANF Autoridad de Certificacion*
Issuer L:	*Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*
Issuer ST:	*Barcelona*
Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-G63287510*
Subject CN:	*ANF AC Servicio de conservación*
Subject E:	*soporte@anf.es*
Subject OU:	*Certificado Cualificado de Sello Electronico*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona*
Subject ST:	*Cataluña*
Subject C:	*ES*
Valid from:	*Thu Dec 03 11:01:00 CET 2020*
Valid to:	*Sat Dec 03 11:01:00 CET 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A5:3E:E0:35:E6:74:20:1D:4A:18:85:DF:3E:B1:50:DA:79:DA:78:19:B1:6D:E1:EC:D4:7D:E3:E8:B6:1A:D4:90:95:2B:F6:94:6B:CF:8F:FB:13:41:DB:0D:3D:0A:9D:3A:16:AA:B4:93:4C:2E:81:30:F7:FE:FF:52:3D:3C:8C:7A:02:EE:72:D9:4E:AE:4D:94:D6:82:D8:95:40:1C:51:1E:DD:A9:E9:61:44:8C:74:4F:2D:67:D7:5D:16:B0:AF:1B:20:22:9F:08:B8:BF:B2:26:E7:D1:C1:EA:E7:79:A5:D9:AD:B8:14:07:62:C5:96:B4:60:B9:18:2B:3E:53:7B:9F:39:A3:55:0A:8A:56:74:89:2E:9A:29:25:78:04:C9:8F:2B:A8:2B:4C:52:42:18:C3:69:6F:15:AC:A7:DF:59:3A:FA:EE:66:B8:FF:CD:E2:A0:38:E0:EB:6E:4E:6A:3C:D8:E7:5E:DE:78:EC:FA:98:E2:3F:E3:09:9E:2D:B2:76:69:B5:CA:B0:B0:E6:0E:40:7E:04:1A:2B:AD:57:37:4C:3F:9F:3D:CB:30:FD:94:F3:1A:38:72:4D:C5:BE:9E:DE:55:10:CE:C8:23:8F:B9:10:89:FD:FA:AF:6D:83:9B:03:C7:4B:EB:08:56:15:DD:D1:46:21:65:C1:D4:F7:63:E5:5F:02:03:01:00:01*
Authority Key Identifier	*35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*
Subject Key Identifier	*11:5E:8B:8B:62:23:EB:73:D1:95:0B:C6:F8:05:EE:A3:FB:16:92:53*
Subject Alternative Name	*soporte@anf.es*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.18332.25.1.1.1* *CPS pointer: https://www.anf.es/documentos* *Policy OID: 0.4.0.194112.1.1*

Authority Info Access	*http://ocsp.anf.es/spain/AV* *http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer*
Basic Constraints	*IsCA: false*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*54:AC:F8:77:4B:6F:AB:83:7B:AB:F5:47:3E:C7:8B:13:85:7E:5E:D1:D7:D5:9F:30:B3:5C:9C:EA:3E:9F:C8:62*

X509SubjectName

Subject 2.5.4.97:	*VATES-G63287510*
Subject CN:	*ANF AC Servicio de conservación*
Subject E:	*soporte@anf.es*
Subject OU:	*Certificado Cualificado de Sello Electronico*
Subject O:	*ANF Autoridad de Certificacion*
Subject L:	*Barcelona*
Subject ST:	*Cataluña*
Subject C:	*ES*

X509SKI

X509 SK I	*EV6Li2Ij63PRlQvG+AXuo/sWklM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2021-03-17T01:00:00Z*

6.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.11.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.12 - Service (granted): Qualified Certificates issued by ANF Secure Server CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by ANF Secure Server CA*
Name	*[es]*	*Servicio de certificados cualificados emitidos por ANF Secure Server CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *99621228724240982512877786 67*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHdjCCBV6gAwIBAgIMIDB5kwrgbnZAv1VrMA0GCSqGSIb3DQEBCwUAMIGEMRIwEAYDVQQFEwlH
NjMyODc1MTAxCzAJBgNVBAYTAkVTMScwJQYDVQQKEx5BTkYgQXV0b3JpZGFkIGRlIlENlcnRpZmlj
YWNpb24xFDASBgNVBAsTC0FORiBDQSBSYWl6MSIwIAYDVQQDExlBTkYgU2VjdXJlIlFNlcnZlciBS
b290IENBMB4XDTIwMTEwOTEyNDcyMloXDTMwMTEwNzEyNDcyMlowgZUxEjAQBgNVBAUTCUc2MzI4
NzUxMDELMAkGA1UEBhMCRVMxJzAlBgNVBAoTHkFORiBBdXRocmlkYWQgZGUgQ2VydGlmaWNhYl2lv
bjEqMCgGA1UECxMhQU5GIEF1dG9yaWRhZCBpbnRlcm1lZGlhIHRlY25pY29zMR0wGwYDVQQDExRB
TkYgU2VjdXJlIlFNlcnZlciBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAOH0SNW2
co+gPghAZHu2eAIqHh5JHAbPMf+x3B2LLEtIVc0/J4mD/Z7XnH5wAml+NK5GkHFJfKIgkHDPUj
7C43kKOxwgL2OmYqgnviVnc/ZHA/49CYQQQFd+k+wTj9PjK6kwobbf6L6/TIfjCPJXwXQjrT8L
BgY9uAWSpuaxCWzAFiF/D7wCOzMdJoa9gpvCRyX+D1qdNmcXX94+fjEN0Bu60mf5Ax3199H1
Rf+etuTMWWflE3l+86kqiiqNjUsuptwrxVteMRtOrCP2H/ZXQaZ89ThIYeEnLyyj1FMuehv22Ny
9bFTbTwAJtk/4JWv16GhkzP9ZM4vvhSm4UUufeKIvVjakrX4Uf8X9gty2D6czrvHpjz7vNm5EvIa
yAMDmbmt9Qw0jhmnRgSRY9jHuXNoqFO8cfgXsRcjBFM7PythxgbNbzGveRUvxk+uzBWibMPJDWk
waSomCvZwWEVasf4wMFhIv78KcQnqEPwBCZknDd0WAdtKKMeN91zPwViEiq8RTHcGp7IbAVmED5
x0WJ/CilEzhQp1AKlJ2ljLGP9rgSrIlc291A8/NMFE4RXe11VOxyhgmf1RjKP4+XRl+PTZ6xi8/P
Cm3pwcK+8hRoieOetos4pu6gywb3/WdVYzM/6b+Y2Ujk91ydzylNO3XbYn5ZuRGAFo4xAgMBAAGj
ggHTMIIBzzAfBgNVHSMEGDAWgBScX9BsY6NlkSq1TmAitjleILFzBNzAdBgNVHQ4EFgQUlgKt5Mn5
T7COAuk/q5pm7kzIowDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEF
BQcDAjB/BgNVHR8EeDB2MDmgN6A1hjNodHRwOi8vY3JsLmFuZi5lcy9jcmwvQU5GU2VjdXJlU2Vy
dmVyUm9vdENBLWFybC5jcmwwOaA3oDWGM2h0dHA6Ly93d3cuYW5mLmVzL2NybC9BTkZTZWN1cmVT
ZXJ2ZXJSb290QOEtYXJsLmNybDBABgNVHSAEOTA3MDUGBFUdIAAwLTArBggrBgEFBQcCARYfaHR0
cDov L3d3dy5hbmYuZXMvZXMvZG9jdW1lbnRvcnC BtQYIKwYBBQUHAQEtTBTMCxGCCsGAQUFBzAB
hhtodHRwOi8vb2NzcC5hbmYuZXMvc3BhaW4vQVYwUAYIKwYBBQUHMAKGRGh0dHA6Ly93d3cuYW5m
LmVzL2VzL2NlcnRpZmljYXRlcy1kb3dubG9hZC9BTkZTZWN1cmVTZXJ2ZXJSb290Q0EuY2VyMA8G
A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggIBAEKbkTISilBMwq/OrU47BTNbF52kMCIS
AgBC52KTD3IwLA0QmhRtoPZCgq0GiLO8i0KguSDN+TkFjZcJYC9qjt0LFiVwGTe9R1vuHaACVT
6qXWxANwkQc3nOn6YEqpgEos4wdanAGtpk1b+oX6rf11f3bomQJmtZUQSdWR1oJlXqR/SbDb6TC
YF5b8wAB+GtG9qkZE9yY/pcUUnqgo11XuNotpysK603MsdXYBIQK/ZKDMxXdZWotq11DesyR+cgVD
WQVa8zZOfu+U7/noUHnL6cJ2YxuZuwhPFq5/n8F9tOdnGkuhD1T/Ph0JgQ3cRCsHSamZ53+xaGEN
2B6fmexxFedfmS640vobpQRi6b5S+gpgC+ltL1odJRiHwFbECZXH6NZWvQkHDFFjGWAPSLlbn
BXdhXUXMsZcQy7Q2IuOUbwZolCD9QMenqeGIgCBLqx1/WgKrTYcyt2DmwNW0YPtjrGhHVCieGUQO
Zrlo88C1W/pO4lS0bj0CB0dojL4dzJ60gM1NHBAQvXbVQNxEUC9ugORbSyezJSU6wRrhZDsXH7o
oiW2UXaL V2RoxGYbAs+dELur1ZtD/l9HVnbZTLwZYzD77Cy80TFl7cS8QvaGwFGRJlxHWkQeKOAR
w31YVsDapNH0qM5hatEd1oKghbyIlHZ3Iakw24iegOCO

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF Secure Server Root CA*

Issuer OU: *ANF CA Raiz*

Issuer O: *ANF Autoridad de Certificacion*

Issuer C: *ES*

Issuer SERIAL NUMBER:	*G63287510*
Subject CN:	*ANF Secure Server CA*
Subject OU:	*ANF Autoridad intermedia tecnicos*
Subject O:	*ANF Autoridad de Certificacion*
Subject C:	*ES*
Subject SERIAL NUMBER:	*G63287510*
Valid from:	*Mon Nov 09 13:47:22 CET 2020*
Valid to:	*Thu Nov 07 13:47:22 CET 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:E1:F4:48:D5:B6:72:8F:A0:3E:08:40:64:7B:B6:78:09:6A:1E:1E:49:1C:06:CF:31:FF:B1:DC:1D:8B:2C:47:C8:55:CD:3F:27:89:83:FD:9E:D7:9C:7E:70:02:69:7E:34:AE:46:90:71:49:7C:A9:1F:82:39:07:0C:F5:23:EC:2E:37:E0:A3:B1:C2:02:F6:3A:66:2A:82:7B:E2:89:59:DC:FD:91:C0:FF:8F:FD:09:84:10:40:57:7E:93:EC:13:8F:D3:E3:2B:A9:30:A1:B6:DF:E8:BE:BF:4E:57:EA:08:F2:57:C1:74:23:89:3F:0B:06:06:1F:F6:EF:00:5B:9A:6E:6B:18:82:5A:B0:05:88:5F:C3:EF:00:8E:CC:C7:49:A1:AF:60:A7:FB:C2:47:25:FE:0F:5A:9D:36:67:17:5F:DE:3E:22:31:0D:D0:1B:BA:D2:67:F9:03:1D:F5:F7:D1:F5:46:BF:9E:B6:E4:CC:59:67:E5:13:79:7E:F3:A9:2A:8A:2A:8D:8D:4B:2E:A6:DC:2B:C5:5B:5E:31:1A:CE:AC:23:F6:1F:F6:57:41:A6:59:F3:D4:E1:21:87:84:9C:BC:B2:8F:51:4C:B9:E8:6F:DB:63:72:F5:B1:53:85:3C:00:26:D9:3F:E0:95:AF:23:A1:A1:93:33:FD:64:CE:2F:BE:14:A6:E1:45:2E:7D:E2:A5:BD:58:DA:92:B5:F8:51:FF:17:F6:0B:72:D8:3E:B6:72:BB:C7:A6:3C:FB:BC:D9:B9:12:F2:1A:C8:03:03:99:B9:AD:F5:0C:34:8E:19:E6:46:04:91:63:D8:C7:B9:73:68:A8:53:BC:71:F8:17:B1:17:A3:04:53:3B:3F:2B:61:C5:A8:1B:35:BC:C6:BD:E4:54:BF:19:3E:BB:30:56:B5:B3:0F:24:35:A4:C1:A4:A8:98:2C:99:C1:61:15:6A:CE:B8:C0:C1:61:96:FE:FC:25:C4:1A:A8:43:F0:04:26:64:9C:37:4E:58:07:6D:28:A3:1E:37:D9:75:CC:FC:15:88:48:AA:F1:14:C7:70:6A:7B:25:B0:15:98:40:F9:C7:45:89:FC:28:A5:13:38:50:A7:50:0A:94:9D:A5:8C:B1:8F:F6:B8:12:AC:82:1C:DB:DD:40:F3:F3:4C:14:4E:11:5D:ED:75:54:EC:72:86:09:9F:D5:18:CA:3F:8F:97:44:8F:8F:4D:9E:B1:8B:CF:CF:0A:6D:E9:C1:C2:BE:F2:14:68:89:E3:9E:B6:8B:38:A6:EE:A0:CB:06:F7:FD:67:55:63:33:3F:EA:1F:98:D9:48:E4:F7:5C:9D:CF:29:4D:3B:75:E1:62:7E:59:B9:11:80:16:8E:31:02:03:01:00:01*
Authority Key Identifier	*9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37*
Subject Key Identifier	*96:02:AD:E4:C9:F9:4F:B0:AD:38:0B:A4:FE:AE:6C:A6:6E:E4:7C:8A*
Extended Key Usage	*id_kp_serverAuth*
CRL Distribution Points	*http://crl.anf.es/crl/ANFSecureServerRootCA-arl.crl* *http://www.anf.es/crl/ANFSecureServerRootCA-arl.crl*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.anf.es/es/documentos*
Authority Info Access	*http://ocsp.anf.es/spain/AV* *http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer*
Basic Constraints	*IsCA: true*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*30:6B:F8:09:96:36:A4:4F:FF:B5:EE:DC:E6:E3:0C:0F:36:C7:D4:3F:6C:CA:5A:2C:A3:AB:71:66:8F:35:33:20*

X509SubjectName

Subject CN:	*ANF Secure Server CA*
Subject OU:	*ANF Autoridad intermedia tecnicos*

Subject O:	*ANF Autoridad de Certificacion*
Subject C:	*ES*
Subject SERIAL NUMBER:	*G63287510*

X509SKI

X509 SK I	*lgKt5Mn5T7CtOAuk/q5spm7kfIo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2021-03-17T01:00:00Z*

6.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

7 - TSP: Consejo General de la Abogacía Española

.

TSP Name

Name	*[en]*	*Consejo General de la Abogacía Española*
Name	*[es]*	*Consejo General de la Abogacía Española*

TSP Trade Name

Name	*[en]*	*VATES-Q2863006I*
Name	*[en]*	*AC ABOGACÍA*
Name	*[es]*	*AC ABOGACÍA*
Name	*[en]*	*Consejo General de la Abogacia NIF:Q-2863006I*
Name	*[en]*	*Consejo General de la Abogacia NIF Q2863006I*
Name	*[en]*	*Consejo General de la Abogacia*
Name	*[en]*	*CONSEJO GENERAL DE LA ABOGACIA*

PostalAddress

Street Address	*[en]*	*Paseo de Recoletos, 13*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28004*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Paseo de Recoletos, 13*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28004*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.acabogacia.org*
URI	*[en]*	*mailto:info@acabogacia.org*

TSP Information URI

URI	*[en]*	*http://www.acabogacia.org*
URI	*[es]*	*http://www.acabogacia.org*

7.1 - Service (withdrawn): Qualified certificate provided by AC Certificados Corporativos

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificate provided by AC Certificados Corporativos*
Name	*[es]*	*Certificados Reconocidos emitidos por CA AC Certificados Corporativos*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *161146793180004064011629729231987846242*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFSTCCBM2gAwIBAgIQeTu+UknX0v1Cr9hEJpysYjANBgkqhkiG9w0BAQUFADB5MQswCQYDVQQG
EwJFUzE2MDQGA1UEChMtQ29uc2VqbyBHZWS5lcmFsIGRlIGxhIEFib2dhY2lhIE5IRjpRLTI4NjMw
MDZJMTIwMAYDVQQDEylBdXRvcmlkYWQgZGlsaGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTAc
Fw0wNTA2MTUwNzI4MDRaFw0xNzA2MTMyMjAwMDBaMIHWMQswCQYDVQQGEwJFUzEPMA0GA1UEBxMG
TWFkcmlkMSAwHgYJKoZIhvcNAQkBFhFhY0BhY2Fib2dhY2lhLm9yZzE2MDQGA1UEChMtQ29uc2Vq
byBHZW5lcmFsIGRlIGxhIEFib2dhY2lhIE5IRjpRLTI4NjMwMDZJMTIwMAYDVQQLEylBdXRvcmlk
YWQgZGUgQ2VydGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTEoMCYGA1UEAxMfQUNBIC0gQ2VydGlm
aWNhZG9zIENvcnBvcmFtaXZvczCCASNwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1G0BQM
h6yK0XZmNVdzEb12qtmppYM0qio1Nopby4NpWDlcr0HD92+zlQjv1FRPjGMVhkH11Vinfss4teyQn
U3U9uwKNjK18DLToZGnersiCcaxxzGunsNLglMEcpmXJHhQrpGc3MhovRGklK0OilinkArYcBE08
/q2zG8mgg1szZ5kwwrZmr2tfS6N9VwBYUeY+VSCpJcUCKQ6AnX8mknbLcZ0nnr2pvtyvrT28Jh
BgVig/iAlJZco/MbUDkkJcIM9K3dcxOZYdfT1VqfIO4oV46ptHGcfKAHMK9u2wJnL1ybGDtCMGO8+S
j25FQz/GO8yeWklzAirln2arl9tXXasCAwEAAaOCAgkwggIFMDcGA1UdEgQwMC6BEWFjQGFjYWJv
Z2FjaWEub3JnhhlodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnMDcGA1UdEQQwMC6BEWFjQGFjYWJv
Z2FjaWEub3JnhhlodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIAHzAdBgNVHQ4EFgQUWnIMoQs8CBYywoVFTzKr
5ytFwBEwHwYDVR0jBBgwFoAUlhMjm0EoSCQ0/gcmrNnBF95gMYwga8GA1UdIASBpzCBpDCBoQYL
KwYBBAGBgRUKAQEwgZEwLQYIKwYBBQUHAgEWIXVyaTpodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3Jn
L2RvYzBgBggrBgEFBQcCAjBUGlJDb25zdWx0ZSBsYSBkZWNsYXJhY2lvbiBkZSBwcmFjdGljYXMg
ZGUgY2VydGlmaWNhY2lvbiBlbiBodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnMGsGA1UdHwRkMGIw
YKBeoFyGLGh0dHA6Ly93d3cuYWNhYm9nYWNpYS5vcmcvY3Js1.2FjYWJvZ2FjaWEuY3JshixodHRw
Oi8vY3JsLmFjYWJvZ2FjaWEub3JnL2NybC9hY2Fib2dhY2lhLmNybDANBgkqhkiG9w0BAQUFAAOC
AQEAUvrnCla/agJC0K41RUNCFA2Hyyl7XOJFwuww/KkRY+w/YkBz5PPfMdmWJRUqWixOwal510I
rYkzvIpQWwILRHwvg+GI5yYtJCYfie63uRa/nFjEL2EfJDZfdTwJLqmjkSrV5gb94AM7n8I3bqI
hAFGBUwhLJWqMU8B294+0MQVo9pHVxJzdchjFLkjfVI5b4QuSJgpWSk7fghfiN40b8TWZzH1IncO
B1yu6vq4RQY9LiZ/mz+VFo+uT8l5N0ETm1b5oCumGFOSGAB7Aic0ZUf4eBH6LrOeBCmj1zTouwv6
KtWvBwNBSsnivm09J6OUh5Aj45VmbjYFvplpJQGYgGA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Autoridad de Certificacion de la Abogacia*

Issuer O: *Consejo General de la Abogacia NIF:Q-2863006I*

Issuer C: *ES*

Subject CN:	*ACA - Certificados Corporativos*
Subject OU:	*Autoridad de Certificacion de la Abogacia*
Subject O:	*Consejo General de la Abogacia NIF:Q-2863006I*
Subject E:	*ac@acabogacia.org*
Subject L:	*Madrid*
Subject C:	*ES*
Valid from:	*Wed Jun 15 09:28:04 CEST 2005*
Valid to:	*Wed Jun 14 00:00:00 CEST 2017*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:46:D0:14:0C:87:AC:8A:D1:76:66:35:57:73:11:BD:76:AA:D9:A9:A5:83:34:AA:2A:13:36:8A:5B:CB:83:69:58:39:5C:AF:41:C3:F7:6F:B3:95:08:EF:D4:54:4F:8C:63:15:86:41:F5:D5:58:A7:86:CE:2D:7B:24:27:53:75:3D:BB:02:8D:8C:AB:7C:0C:B4:E8:64:69:DE:AE:C8:82:71:AC:71:CC:6B:A7:B0:D2:E0:24:C1:1C:A6:65:C9:1E:14:2B:A4:67:37:32:1A:2F:44:69:25:2B:43:A2:96:29:E4:02:B6:1E:04:4D:3C:FE:AD:B3:1B:C8:A7:82:04:FC:CD:9E:64:C3:0A:D9:9A:BD:AD:7D:2E:8D:F5:5C:01:61:47:98:FD:54:82:A4:97:0B:08:A4:3A:02:75:FC:9A:49:DB:2D:C6:74:9E:7A:F6:CA:9B:ED:CA:FC:D3:DB:C2:61:06:05:62:83:F8:80:D1:91:A8:FC:C6:D4:0E:42:89:70:83:3D:2B:77:5C:C4:E6:58:74:52:15:A8:73:B8:A1:5E:3A:A6:D1:C6:79:F2:80:1C:C2:BD:BB:6C:09:9C:BD:7F:CA:11:83:9C:23:06:3B:CF:92:8F:6E:45:43:3F:C6:3B:CC:9E:5A:49:73:02:2A:E5:9F:66:AB:97:DB:57:5D:AB:02:03:01:00:01*
Issuer Alternative Name	*ac@acabogacia.org*
Subject Alternative Name	*ac@acabogacia.org* *http://www.acabogacia.org*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*5A:79:4C:A1:0C:FC:08:16:2C:C2:85:45:4F:32:AB:E7:2B:45:C0:11*
Authority Key Identifier	*FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.16533.10.1.1* *CPS pointer: uri:http://www.acabogacia.org/doc* *CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]*
CRL Distribution Points	*http://www.acabogacia.org/crl/acabogacia.crl* *http://crl.acabogacia.org/crl/acabogacia.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C3:2F:2C:6D:70:6F:AC:23:94:7D:2B:09:21:A4:B5:A6:98:0B:E7:96:BB:2D:D6:F2:11:8E:BA:6D:82:54:A8:FC*

X509SubjectName

Subject CN:	*ACA - Certificados Corporativos*
Subject OU:	*Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject E: *ac@acabogacia.org*

Subject L: *Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-12-04T01:00:00Z*

7.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificate provided by AC Certificados Corporativos*

Name *[es]* *Certificados Reconocidos emitidos por CA AC Certificados Corporativos*

Service digital identities

X509SubjectName

Subject CN: *ACA - Certificados Corporativos*

Subject OU:	*Autoridad de Certificacion de la Abogacia*
Subject O:	*Consejo General de la Abogacia NIF:Q-2863006I*
Subject E:	*ac@acabogacia.org*
Subject L:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*WnlMoQz8CBYswoVFTzKr5ytFwBE=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

7.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service Name		
Name	*[en]*	*Qualified certificate provided by AC Certificados Corporativos*
Name	*[es]*	*Certificados Reconocidos emitidos por CA AC Certificados Corporativos*

Service digital identities

X509SubjectName

Subject CN:	*ACA - Certificados Corporativos*
Subject OU:	*Autoridad de Certificacion de la Abogacia*
Subject O:	*Consejo General de la Abogacia NIF:Q-2863006I*
Subject E:	*ac@acabogacia.org*
Subject L:	*Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*WnlMoQz8CBYswoVFTzKr5ytFwBE=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2007-05-22T00:00:00Z*

7.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.2 - Service (withdrawn): Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía*

Name *[es]* *Certificados Reconocidos emitidos por CA Autoridad de Certificación de la Abogacía*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *136*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGWzCCBUOgAwIBAgICAIgwDQYJKoZIhvcNAQEFBQAwgZ0xCzAJBgNVBAYTAkVTMSIwIAYDVQQH
ExIDLyBNdW50YW5lciAyNDQgQmFyY2Vsb25hMUIwQAYDVQQDEzlBdXRvcmlkYWQgZGUgQ2VydGlm
aWNhY2lvbiBGaXJtYXByb2Zlc2lvbmFsIENJRiBBNjI2MzQwNjgxJjAkBgkqhkiG9w0BCQEWF2Nh
QGZpcm1hcHJvZmVzaW9uYWwuY29tMB4XDTA0MDMwMjA5NDMxMFoXDTEzMDMyNTIzMDAwMFowge4x
CzAJBgNVBAYTAkVTMSAwHgYJKoZIhvcNAQkBFhY0fhN2Fib2dhY2lhLm9yZzElMCMGA1UEBxMc
UGFzZW9gZGU gLmVjb2xkdG9zIDEzIE1hZHIpzDEzMCkGA1UECxMdQ29uc3VsdGUgaHR0cDovL3d3
dy5hY2Fib2dhY2lhLm9yZzE1MDMGA1UEChMsQ29uc2VqbyBHZW5lcmFsIGRlIGxhIEFib2dhY2lh
IE5JRiBRMjg2MzAwNkkxMjAwBgNVBAMTKUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIGRlIGxh
IEFib2dhY2lhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyDAdZbS0WyrPDrnL Upk6
UBhbSI1IA6H5V2l pntQYEJ0CIDIU3Y8PVKmx+rVbRa6vPnO8o4kMnJdyE8tVQghGL/WT3
luB5SVXcU3lxfLt/XHKB6sqk8e/b0anm3eyaZ4vGjcxRBmIofm46PnGMI8eeYwUT3ur3ycILf+5n
sNP26S3i6yWIz6jgmu13Ahp63xMS5JTJDOOkiEgIAMOEY8fE1CY3bCVZi9AzS6PJrVM/8xhWk2C2
TsIBX64APz15BTrlr13zHUREOkcanleeVpOKAwgILcJG0fzZwAMnypfaftKAC7NlM/tFiX39gAB
J2febNfipCbXOfinLQIDAQABo4ICUDCCAkwwKgYDVR0SBCMwIYYfaHR0cDovL3d3dy5maXJtYXBy
b2Zlc2lvbmFsLmNvbTAkBgNVHREEHTAbhhlodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnMBIGA1Ud
EwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIABzA6BglghkgB
hvhCAQgELRYraHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbS9jcHMvY3BzLmh0bTAdBgNV
HQ4EFgQUlrpZcaxzpBNtPBiv9dC741a9k7AwgeoGA1UdIwSBwjCBv4AUMwugZtHq2s7eYpMEKFK1
FH84aLehgaOkgaAwgZ0xCzAJBgNVBAYTAkVTMSIwIAYDVQQHExIDLyBNdW50YW5lciAyNDQgQmFy
Y2Vsb25hMUIwQAYDVQQDEzlBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbiBGaXJtYXByb2Zlc2lv
bmFsIENJRiBBNjI2MzQwNjgxJjAkBgkqhkiG9w0BCQEWF2NhQGZpcm1hcHJvZmVzaW9uYWwuY29t
ggEBMFIGA1UdIARLMEkwRwYKKwYBBAHmeQoKATA5MDcGCCsGAQUFBwIBFitodHRwOi8vd3d3LmZp
cm1hcHJvZmVzaW9uYWwuY29tL2Nwcy9lcHMuaHRtMEUGA1UdHwQ+MDwwOqAoOaGNGb0dHJAdLy9j
cmwuZmlybWFwcm9mZXNpb25hbC5jb20vZmlybWFwcm9mZXNpb25hbC5jcmwwDQYJKoZIhvcNAQEF
BQADggEBAEgEBIMEkqLzsxQ5zmx048XwDe5NnBvBBJPMz/HQ2P4zKiqun4wyQObbXYxJcVUOHJbZ
e4FBGHeRWcfCOkt6VHgGCCW6DgBD8jZmV5cDqYMFxpXLHlA/L8EKu7ch6NSf230zC+0/cO/1KO4
kwW0nhZmtrDkX9z9xRobyYcmC7wEQAca6i1qc0Hp9pQp70vRsZio07vLHZz1VOQuJwmp/cpU6ll
y+pGmqWlsBCXSWAjq+q3ZJ4wKWFbtBt8kiuvSGfaOahfE35+/hXtgdIjxsDK5lh1uNR9ho5aUhLu
T1lvNeDPKG2RQM03bAPcEzcWno101drtKwkmPhjpsWr3iIF=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer E: *ca@firmaprofesional.com*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer L: *C/ Muntaner 244 Barcelona*

Issuer C: *ES*

Subject CN: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF Q2863006I*

Subject OU: *Consulte http://www.acabogacia.org*

Subject L: *Paseo de Recoletos 13 Madrid*

Subject E: *ac@acabogacia.org*

Subject C: *ES*

Valid from: *Tue Mar 02 10:43:10 CET 2004*

Valid to: *Tue Mar 26 00:00:00 CET 2013*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:30:1D:65:B4:B4:5B:2A:CF:0E:B9:CB:52:99:3A:50:18:A1:F1:2D:5F:D6:50:3A:1F:95:76:2E:99:D0:60:42:7F:38:2
2:03:7D:4F:D8:F0:F5:4A:9B:1F:BE:AD:58:A1:45:AE:BF:BC:F9:CE:B6:8E:24:B4:C2:27:25:DC:84:F2:D5:50:82:11:8B:FD:61:77:96:E0:79:49:55:DC:53:79:71:7C:BB:7F:5C:72:81:EA:CA:A4:F1:EF:DB:D1:A9:E6:DD:EC:9
A:67:8B:C6:8D:CC:51:06:62:28:7E:6E:3A:3E:71:8C:23:C7:9E:63:05:13:DE:EA:F7:C9:C2:0B:7F:EE:67:B0:D3:F6:E9:2D:E2:EB:25:88:CF:A8:E0:9A:ED:77:02:1A:7A:DF:13:12:E4:94:C9:0C:E3:A4:88:48:00:C3:84:63:C
7:C4:D4:26:37:6C:25:59:8B:D0:33:4B:A3:C9:AD:53:3F:F3:18:56:93:60:B6:4E:C7:C1:5F:AE:00:3F:3D:79:05:3A:E5:AF:5D:F3:1D:44:44:3A:47:1A:9E:57:9E:56:93:8A:03:08:25:2D:C2:46:D1:FC:D9:C0:03:27:CA:9D:1A:7E
:DB:4A:00:2E:CD:94:CF:ED:16:25:F7:F6:00:01:27:67:DE:6C:D7:EC:A4:26:D7:39:F8:B1:2D:02:03:01:00:01
```


Issuer Alternative Name *http://www.firmaprofesional.com*

Subject Alternative Name	*http://www.acabogacia.org*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*22:BA:59:71:AC:73:A4:13:6D:3C:18:AF:F5:D0:82:E3:56:BD:93:B0*
Authority Key Identifier	*33:0B:A0:66:D1:EA:DA:CE:DE:62:93:04:28:52:B5:14:7F:38:68:B7*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.13177.10.10.1* *CPS pointer: http://www.firmaprofesional.com/cps/cps.htm*
CRL Distribution Points	*http://crl.firmaprofesional.com/firmaprofesional.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*BC:85:94:4D:A4:E3:04:E9:B7:05:8A:19:B6:73:AF:95:F5:40:D0:0D:CD:A0:10:90:3A:00:9D:A2:FB:AC:AB:6E*

X509SubjectName

Subject CN:	*Autoridad de Certificacion de la Abogacia*
Subject O:	*Consejo General de la Abogacia NIF Q2863006I*
Subject OU:	*Consulte http://www.acabogacia.org*
Subject L:	*Paseo de Recoletos 13 Madrid*
Subject E:	*ac@acabogacia.org*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

7.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.2.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía*

Name *[es]* *Certificados Reconocidos emitidos por CA Autoridad de Certificación de la Abogacía*

Service digital identities

X509SubjectName

Subject CN: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF Q2863006I*

Subject OU: *Consulte http://www.acabogacia.org*

Subject L: *Paseo de Recoletos 13 Madrid*

Subject E: *ac@acabogacia.org*

Subject C: *ES*

X509SKI

X509 SK I *IrpZcaxzpBNtPBiv9dCC41a9k7A=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2007-05-21T22:00:00Z*

7.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía*

Name *[es]* *Certificados Reconocidos emitidos por CA Autoridad de Certificación de la Abogacía*

Service digital identities

X509SubjectName

Subject CN: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF Q2863006I*

Subject OU: *Consulte http://www.acabogacia.org*

Subject L: *Paseo de Recoletos 13 Madrid*

Subject E: *ac@acabogacia.org*

Subject C: *ES*

X509SKI

X509 SK I *IrpZcaxzpBNtPBiv9dCC41a9k7A=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

7.3 - Service (withdrawn): Qualified Certificates issued by ACA Trusted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by ACA Trusted*

Name *[es]* *Certificados Reconocidos emitidos por CA ACA Trusted*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *451196096372053263385677474235762321 29*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFvDCCBKSgAwIBAgIQIfG4gaBA/hxKJQICBy+QwTANBgkqhkiG9w0BAQUFADB5MQswCQYDVQQG
EwJFUzE2MDQGA1UEChMtQ29uc2VqbyBHZWS5lcmFsIGRlIGxhIEFib2dhY2lhIE5JRjpRLTI4NjMw
MDZJMTIwMAYDVQQDEylBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTAe
Fw0wOTA2MDIxMDQyMTBaFw0yOTA2MDEyMjAwMDBaMIHAMQswCQYDVQQGEwJFUzEgMB4GCSqGSIb3
DQEJARYRY2FAYWNhYm9nYWNpYS5vcmcxMjAwBgNVBAsTKUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2Fj
aW9uIGRlIGxhIEFib2dhY2lhMTYwNAYDVQQKEy1Db25zZWpvIEdlbmVyYWwgZGUgbGEgQWJvZ2Fj
aWEgTkIGOlEtMjg2MzAwNkxJzAhBgNVBAMTGkFDQSAtIFRydXN0ZWQgQ2VydGlmaWNhdGVzMlIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs3mfQ+XQAbBI1kVhpsDTasMPuuGQTbEbA0C8
ohHb2GOxsMBK5HMaxHp3pnGCL2mzb8jURPds1MWVbdrO5HOXE3g/oot154wyqmcj1p7jOLeePzVX
WCn5pAHqS9kEfx6dI3inQokkZaX2EukbGnU0Xvyb69FsDbZYw6Za67QRP4Bnz0LcuoFN7M2BJ8MA
2MhMASBDpr+6hBkqxoOliUMmYcDbR7dYltb/V+ZpoIcAlmbq+J1OZr8nZX6TbBgjxDffs5wMSDP1
UDSt5xwjKkmZk0YbNKcNfpSxATT2TVTyaUGBKZ6wQ3tbCLtaho0rEvRZecpbke897YSs6tAkLxyT
+wIDAQABo4IB9jCCAfIwNwYDVR0SBDAwLoERYWNAYWNhYm9nYWNpYS5vcmcGGWh0dHA6Ly93d3cu
YWNhYm9nYWNpYS5vcmcwJAYDVR0RBB0wG4YZaHR0cDovL3d3dy5hY2Fib2dhY2lhLm9yZzAPBgNV
HRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjARBglghkgBhvhCAQEEBAMCAAcwHQYDVR0OBBYE
FFr2NMe6Wdla3fOmc3B0TbHneDzB2MB8GA1UdIwQYMBaAFPyITSt8KEgkNP4HJqzZwRteYDGMIGv
BgNVHSAEgacwgaQwgaEGCysGAQQBgYEVCgEBMIGRMC0GCCsGAQUFBwIBFiFlcmktaHR0cDovL3d3
dy5hY2Fib2dhY2lhLm9yZy9kb2MwYAYIKwYBBQUHAgIwVBpSQ29uc3VsdGUgbGEgZGVibGFyYWNp
b24gZGUgcHJhY3RpY2FzIGRlIGNlcnRpZmlyYWNpb24gZW4gaHR0cDovL3d3dy5hY2Fib2dhY2lh
Lm9yZzBrBgNVHREZDBiMGCgXqBchixodHRwOi8vd3d3LmFyYWJvZ2FjaWEub3JnL2NybC9hY2Fi
b2dhY2lhLmNybHYsaHR0cDovL2NybC5hY2Fib2dhY2lhLm9yZy9jcmwvYWNhYm9nYWNpYS5jcmww
DQYJKoZIhvcNAQEFBQADggEBAIE5IgwYEm8Z4IRIJe9nwytDlNiXQMLrORikXI7efKqcELOlrNCu
LuWM94ekeUjbWG4L7Qp1Z+KMnCDf0uc+v51a3EHUKRQeucZkEuZybejDShLS9K7WQOBYiVIkZWeU
tOkLnUAyT1w4LNLiFsdMhcYLLcsZmkWLD8+toIOcGZSMThENRJW0BjZ+agT+aE9TrnJlaIUDdqm
8gTi1wR/nygMphzD/u3kxRvAUVwez0VpLanNJ0Qp+FLJAbH1PzkvYWBiG1bQUFUby5J9NPYQwKI
4DxCiDRLNcMbUiwZrAdoHLQvPM9HF3asxgQH4GOLCdZE9cXfvQ7au0wvqc2TTns=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN:	*Autoridad de Certificacion de la Abogacia*
Issuer O:	*Consejo General de la Abogacia NIF:Q-2863006I*
Issuer C:	*ES*
Subject CN:	*ACA - Trusted Certificates*
Subject O:	*Consejo General de la Abogacia NIF:Q-2863006I*
Subject OU:	*Autoridad de Certificacion de la Abogacia*
Subject E:	*ca@acabogacia.org*
Subject C:	*ES*
Valid from:	*Tue Jun 02 12:42:10 CEST 2009*
Valid to:	*Sat Jun 02 00:00:00 CEST 2029*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B3:79:9F:43:E5:D0:01:B0:65:D6:45:5B:A6:20:D3:6A:C3:0F:BA:E1:90:4E:11:21:03:40:BC:A2:11:DB:D8:63:B1:B0:C0:4A:E4:73:1A:C4:7A:77:A6:21:82:2F:69:B3:87:C8:D4:44:F7:6C:D4:C5:95:6D:DA:CE:E4:73:97:13:78:3F:A2:8B:75:E7:8C:32:AA:67:23:D6:9E:E3:38:B7:9E:3F:35:57:58:29:F9:A4:01:EA:4B:D9:04:7F:1E:9D:7F:78:A7:42:89:24:65:A5:F6:12:E9:1B:1A:75:34:5E:FC:9B:EB:D1:6C:0D:B6:58:C3:A6:5A:EB:B4:11:3F:80:67:CF:42:DC:BA:81:4D:EC:CD:81:27:C3:00:D8:C8:4C:01:20:43:A6:BF:BA:84:19:2A:C6:83:88:89:43:26:61:C0:DB:47:B7:58:22:D6:FF:57:E6:69:A1:F7:00:96:66:EA:F8:9D:4E:66:BF:27:65:7E:93:6C:18:23:C4:37:DF:B3:9C:0C:48:33:F5:50:34:AD:E7:1C:23:2A:49:99:93:46:21:34:A7:0D:7E:94:B1:01:31:76:4D:54:F2:69:41:81:29:9E:B0:43:7B:5B:08:BB:5A:86:8D:2B:12:FF:19:79:CA:5B:91:EF:3D:ED:84:AC:EA:D0:24:2F:1C:93:FB:02:03:01:00:01*
Issuer Alternative Name	*ac@acabogacia.org*
Subject Alternative Name	*http://www.acabogacia.org*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*5A:F6:34:CE:96:76:56:B7:7C:E9:DC:DC:1D:13:6C:79:DE:0F:30:76*
Authority Key Identifier	*FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.16533.10.1.1* *CPS pointer: uri:http://www.acabogacia.org/doc* *CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]*
CRL Distribution Points	*http://www.acabogacia.org/crl/acabogacia.crl* *http://crl.acabogacia.org/crl/acabogacia.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*68:07:A3:F3:7B:3C:6C:18:07:48:52:65:73:0B:BE:3F:6A:37:86:6F:34:8F:5E:F2:12:3C:E8:63:77:38:E0:FC*

X509SubjectName

Subject CN:	*ACA - Trusted Certificates*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject E: *ca@acabogacia.org*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-12-04T01:00:00Z*

7.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ACA Trusted*

Name *[es]* *Certificados Reconocidos emitidos por CA ACA Trusted*

Service digital identities

X509SubjectName

Subject CN: *ACA - Trusted Certificates*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject E: *ca@acabogacia.org*

Subject C: *ES*

X509SKI

X509 SK I *WvY0zpZ2Vrd86dzcHRNsed4PMHY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

7.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ACA Trusted*

Name *[es]* *Certificados Reconocidos emitidos por CA ACA Trusted*

Service digital identities

X509SubjectName

Subject CN: *ACA - Trusted Certificates*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject E: *ca@acabogacia.org*

Subject C: *ES*

X509SKI

X509 SK I *WvY0zpZ2Vrd86dzcHRNsed4PMHY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-09-27T22:00:00Z*

7.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.4 - Service (withdrawn): Qualified certificate provided by AC Certificados Corporativos 2014

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificate provided by AC Certificados Corporativos 2014*

Name *[es]* *Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014*

Service digital identities

Certificate fields details

Version:

3

Serial Number:

50277584362934511984483198896977516751

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFbjCCBFagAwIBAgIQJdMcS2fiqsgBWFR3GcfSYzzANBgkqhkiG9w0BAQsFADB5MQswCQYDVQQG
EwJFUzE2MDQGA1UEChMtQ29uc2VqbyBHZWSlcmFsIGRlIGxhIEFib2dhY2lhIE5JRjpRLTI4NjMw
MDZJMTIwMAYDVQQDEylBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTAe
Fw0xNTEwMDcxMzI3MzRaFw0yNTEwMDcxMzI3MzRaMIGvMQswCQYDVQQGEwJFUzEnMCUGA1UECgwe
Q29uc2VqbyBHZWSlcmFsIGRlIGxhIEFib2dhY2lhMTIwMAYDVQQLDClBdXRvcmlkYWQgZGUgQ2Vy
dGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTESMBAGA1UEBRMJUTI4NjMwMDZJMS8wLQYDVQQDDCZB
Q0EgLSBDZXJ0aWZpY2Fkb3MgQ29ycG9yYXRpdm9zIC0gMjAxNDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALD6GARgl/vrG0Q5VgUw84rxTiG7KSdssuu16l5WWaDI7sjmHrm/qYdJLAuz
x9HzVM2qpnRJDEzR5bmisBKGL3wwtaLPlOBS1+6XrtdIcjMDUy2yFFY9phkdJKlcblHOsmjRQn
jbSEWHbNnf03TolAFcxwwqlO70IRQhJHIAAw1f6zz6cD79Za73u+Azp0TyHnuu88bXKpd324Krmi
cNp1t2MO+9PFC6Rs8h+gwTAmxt1p1vsvLx3+urkwJg1aEdQuXBK7m5qZmn1Gz42B1yD4ZKntBL5
GNXGtkegH94vrqMq2fXvuRnCVczw5M5xWp78OD67n9CviP0V6qDPKjkCAwEAAaOCAbkwggG1MDcG
A1UdEgQwMC6BEWFjQGFjYWJvZ2FjaWEub3JnLnhhlodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnMA8G
A1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBQzbdDpzRjXtOt0/PPjzfs9
W8CjnjAfBgNVHSMEGDAWgBT8iEyObQShIDT+Byas2cEX3mAxjCBqwYDVR0gBIGjMIGgMIGdBgsr
BgEEAYGBFQoBATCBjTApBggrBgEFBQcCARYdaHR0cDovL3d3dy5hY2Fib2dhY2lhLm9yZy9kb2Mw
YAYIKwYBBQUHAgIwVBpSQ29uc3VsdGUgbGEgZGVlbGFyYWNpb24gZGUgcHlhY3RpY2FzIGRlIGNl
cnRpZmlYWNpb24gZWdqaHR0cDovL3d3dy5hY2Fib2dhY2lhLm9yZzBtBgNVHR8EZDBiMGCgXqBc
hixodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2NybC9hY2Fib2dhY2lhLmNybIYsaHR0cDovL2Ny
bC5hY2Fib2dhY2lhLm9yZy9jcmwvYWNhYm9nYWNpYS5jcmwwDQYJKoZIhvcNAQELBQADggEBAG5c
zRpo4MsYnFdLjd1+N0tra7Qaj1xA68UMY2QCalhBpCjlqJ/xEFWnl7vAHARQ65CEUECmr7gGFKHG
VxFca7X/TGkDhN8XzCouYBdwiD4lrbnvUuByVLDo+60bXPzkhWPt4Tbl/wJSBjutyuT7jF+ncIAd2
/xyvFENwb+5pFxw/naM8MvUlGgtSoAvXOrmjjHvNgvdTCEmRziEnqqM3E2msRGQ+PWvdTGHHRF
xkLOR7bXymPtR63fO0VmdLZUey69DD1CIVC0vWkLyVSZENhJjB7JbZ0qUnGN7Kx0CDs0OEp4mzz1
fQxX4h8pG0asWBxQ0u3OEohZIbUFnyhZbw8=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer CN:

Autoridad de Certificacion de la Abogacia

Issuer O:

Consejo General de la Abogacia NIF:Q-2863006I

Issuer C:

ES

Subject CN:

ACA - Certificados Corporativos - 2014

Subject SERIAL NUMBER:

Q2863006I

Subject OU:

Autoridad de Certificacion de la Abogacia

Subject O:

Consejo General de la Abogacia

Subject C:

ES

Valid from:

Wed Oct 07 15:27:34 CEST 2015

Valid to:

Tue Oct 07 15:27:34 CEST 2025

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:FA:18:04:60:97:FB:EB:1B:44:39:56:05:30:F3:8A:F1:4D:F1:BF:29:27:6C:B2:EB:B5:E8:8E:56:5A:E0:C8:EE:C8:E
6:1E:B9:BF:A9:87:49:2C:0B:B3:C7:D1:F3:54:CD:AA:A6:74:49:0C:4C:D1:E5:B9:A2:B0:12:86:2F:7C:30:7D:A2:CF:94:E6:D2:D7:EE:97:AE:D7:48:72:33:03:94:9C:B6:C8:51:58:F6:98:7C:74:92:8A:95:C6:E5:1C:EB:26:8D:1
4:27:8D:B4:B4:58:76:CD:9D:FD:37:4E:89:40:15:EC:70:C2:A9:4E:EF:47:D1:42:12:47:20:00:30:D5:FE:B3:CF:A7:03:EF:D6:5A:EF:7B:BE:02:AC:F4:4F:21:E7:BA:EF:3C:6D:72:A9:77:7D:B8:2A:B9:A2:70:DA:75:B7:FD:8C:
3B:EF:4F:14:2E:91:B3:C8:7E:83:04:C0:9B:1B:75:A7:5B:EC:BC:BC:77:FA:EA:E4:C0:98:35:68:47:50:B9:70:4A:EE:6E:6A:66:69:F5:1B:3E:36:07:5C:83:E1:92:A7:B4:12:F9:18:D5:C6:B6:47:A0:1F:DE:2F:AE:A3:2A:D9:F5:
EF:B9:19:C2:55:EC:F0:E4:CE:71:5A:9E:FC:38:3E:BB:9F:D0:AF:88:FD:15:EA:A0:CF:2A:39:02:03:01:00:01
```


Issuer Alternative Name

ac@acabogacia.org

Basic Constraints

IsCA: true

Subject Key Identifier

33:6D:D0:E9:CD:18:D7:B4:EB:4E:FC:F3:E3:CD:FB:3D:5B:C0:A3:9E

Authority Key Identifier

FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6

Certificate Policies

Policy OID: 1.3.6.1.4.1.16533.10.1.1

CPS pointer: http://www.acabogacia.org/doc

CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]

CRL Distribution Points

http://www.acabogacia.org/crl/acabogacia.crl

http://crl.acabogacia.org/crl/acabogacia.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

7D:42:0E:6C:7F:F1:45:AF:B1:CB:67:2A:55:2E:2F:31:2F:9D:78:58:DC:1D:41:78:09:DC:58:6B:8C:A4:37:3C

Certificate fields details

Version:

3

Serial Number:

42935637685871718833877496530669538074

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFTDCCBDSgAwIBAgIQIE0aYC2KOl9TF1d66lYLGjANBgkqhkiG9w0BAQUFADB5MQswCQYDVQQG
EwJFUzE2MDQGA1UEChMtQ29uc2VqbyBHZWS5lcmFsIGRlIGxhIEFib2dhY2lhIE5JRjpRLTI4NjMw
MDZJMTIwMAYDVQQDEylBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTAe
FwOxNDAzMDUxNjU3MzRaFwOzMDAzMDUxNjU3MzRaMIGvMQswCQYDVQQGEwJFUzEnMCUGA1UECgwe
Q29uc2VqbyBHZW5lcmFsIGRlIGxhIEFib2dhY2lhMTIwMAYDVQQLDClBdXRvcmlkYWQgZGUgQ2Vy
dGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTESMBAGA1UEBRMJUT14NjMwMDZJMS8wLQYDVQQDDCZB
Q0EgLSBDZXJ0aWZpY2Fkb3MgQ29ycG9yYXRpdm9zIC0gMjAxNDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALD6GARgl/vrG0Q5YgUlw84rxTfG/KSdssuu16f5WWuDl7sjmHrmiqYdJLAuz
x9HzVM2qpnRJDE2zR5bmisBKGL3wwfaLPlOfS1+6XrtdIcyMDJy2yFFY9ph8dJKKlcblHOsmjRQn
jbSEWHbNnf03TolAFexwwqIO70fRQhJHIAAw1f6zz6cD79Za73u+Aqz0TyHnuu88bXKpd324Krmi
cNp1t/2MO+9PFC6Rs8b+gwTAmxt1p1vsvLx3+urkwJg1aEdQuXBK7m5qZmn1Gz42B1yD4ZKntBL5
GNXGikzgH94vrqMq2DXvuRntCVzznrSM5xWp78OD67n9CvPf0V6qDPKjkCAwEAAaOCAZcwggGTMA8G
A1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIABzAdBgNVHQ4E
FgQUM23Q6c0Y17TrTvzz4837PVvAo54wHwYDVR0jBBgwFoAU/IhMjm0EoSCQ0/gcmrNnBF95gMYw
ga8GA1UdIASBpzCBpDCBoQYLKwYBBAGBgRUKAQEwgZEwLQYIKwYBBQUHAgEWIXVyaTpodHRwOi8v
d3d3LmFjYWJvZ2FjaWEub3JnL2Rv YzBgBggrBgEFBQcCAjBUGlJDb25zdWx0ZSBsYSBkZWNsYXJh
Y2lvbiBkZSBwcmFzGiljYXMgZGUgY2VydGlmaWNhY2lvbiBlbnBodHRwOi8vd3d3LmFjYWJvZ2Fj
aWEub3JnMGsGA1UdHwRkMGIwYKBeoFyGLGh0dHA6Ly93d3cuYWNhYm9nYWNpYS5vcmcvY3JsL2Fj
YWJvZ2FjaWEuY3JshxodHRwOi8vY3JsLmFjYWJvZ2FjaWEub3JnL2NybC9hY2Fib2dhY2lhLmNy
bDANBgkqhkiG9w0BAQUFAAOCAQEAdSJfnbBYJi8SpwrQq/Lds8QxNKKQSguBy7UvM5/ljFwdS6+d
gc+NT2R1KXC4iuTQHzzta4e6mVfP9MkAwrm3Dgs4bSS+5gxNbucV8Pqreyzd8MuqeSYxBiBgfIC
iuB+rBk2QRslRHk+hZmGDuBo8zdva7djEP6qfifmlWzYJnFPA5h6l3bq6PXfyGF0Ref1EQEG6UKz
DKUqPuIOZLu5yw7944GoyT0Rdj2q/vYF5y4AnzsJOjyxZJKpXijE+5tJFcJB5kYdwAL0QE41mjP5
6dujETzTUgla/8LEH4DbS+1z20H/oBAR0HD3FgvItvLsUpshLjtUjyZCPxcUn2Xx0g==

-----END CERTIFICATE-----
```


Signature algorithm:

SHA1withRSA

Issuer CN:

Autoridad de Certificacion de la Abogacia

Issuer O:

Consejo General de la Abogacia NIF:Q-2863006I

Issuer C:

ES

Subject CN:

ACA - Certificados Corporativos - 2014

Subject SERIAL NUMBER:

Q2863006I

Subject OU:

Autoridad de Certificacion de la Abogacia

Subject O:

Consejo General de la Abogacia

Subject C:

ES

Valid from:

Wed Mar 05 17:57:30 CET 2014

Valid to:

Tue Mar 05 17:57:30 CET 2030

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:FA:18:04:60:97:FB:EB:1B:44:39:56:05:30:F3:8A:F1:4D:F1:BF:29:27:6C:B2:EB:B5:E8:8E:56:5A:E0:C8:EE:C8:E6:1E:B9:BF:A9:87:49:2C:0B:B3:C7:D1:F3:54:CD:AA:A6:74:49:0C:4C:D1:E5:B9:A2:B0:12:86:2F:7C:30:7D:A2:CF:94:E6:D2:D7:EE:97:AE:D7:48:72:33:03:94:9C:B6:C8:51:58:F6:98:7C:74:92:8A:95:C6:E5:1C:EB:26:8D:14:27:8D:B4:84:58:76:CD:9D:FD:37:4E:89:40:15:EC:70:C2:A9:4E:EF:47:D1:42:12:47:20:00:30:D5:FE:B3:CF:A7:03:EF:D6:5A:EF:7B:BE:02:AC:F4:4F:21:E7:BA:EF:3C:6D:72:A9:77:7D:B8:2A:B9:A2:70:DA:75:B7:FD:8C:3B:EF:4F:14:2E:91:B3:C8:7E:83:04:C0:9B:1B:75:A7:5B:FC:BC:BC:77:FA:EA:E4:C0:98:35:68:47:50:B9:70:4A:EE:6E:6A:66:69:F5:1B:3E:36:07:5C:83:E1:92:A7:B4:12:F9:18:D5:C6:B6:47:A0:1F:DE:2F:AE:A3:2A:D9:F5:EF:B9:19:C2:55:EC:F0:E4:CE:71:5A:9E:FC:38:3E:BB:9F:D0:AF:88:FD:15:EA:A0:CF:2A:39:02:03:01:00:01

Basic Constraints

IsCA: true

Subject Key Identifier

33:6D:D0:E9:CD:18:D7:B4:EB:4E:FC:F3:E3:CD:FB:3D:5B:C0:A3:9E

Authority Key Identifier

FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6

Certificate Policies

Policy OID: 1.3.6.1.4.1.16533.10.1.1

CPS pointer: uri:http://www.acabogacia.org/doc

CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]

CRL Distribution Points

http://www.acabogacia.org/crl/acabogacia.crl

http://crl.acabogacia.org/crl/acabogacia.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

5C:DF:25:EE:A9:A1:49:42:F3:4B:38:B8:EA:17:24:2D:DC:53:F8:78:1D:25:A7:8A:98:18:9E:94:E1:69:72:91

X509SubjectName

Subject CN:

ACA - Certificados Corporativos - 2014

Subject SERIAL NUMBER:

Q2863006I

Subject OU:

Autoridad de Certificacion de la Abogacia

Subject O:

Consejo General de la Abogacia

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-12-04T01:00:00Z

7.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.16533.10.5.1

7.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

7.4.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificate provided by AC Certificados Corporativos 2014

Name [es] Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014

Service digital identities

X509SubjectName

Subject CN: ACA - Certificados Corporativos - 2014

Subject SERIAL NUMBER: Q2863006I

Subject OU: Autoridad de Certificacion de la Abogacia

Subject O: Consejo General de la Abogacia

Subject C: ES

X509SKI

X509 SK I M23Q6c0Y17TrTvzz4837PVvAo54=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

7.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificate provided by AC Certificados Corporativos 2014*
Name	*[es]*	*Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014*

Service digital identities

X509SubjectName

Subject CN:	*ACA - Certificados Corporativos - 2014*
Subject SERIAL NUMBER:	*Q2863006I*
Subject OU:	*Autoridad de Certificacion de la Abogacia*
Subject O:	*Consejo General de la Abogacia*
Subject C:	*ES*

X509SKI

X509 SK I	*M23Q6c0Y17TrTvzz4837PVvAo54=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-06-04T22:00:00Z*

7.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.5 - Service (withdrawn): Qualified Certificates issued by ACA Trusted 2014

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en]	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by ACA Trusted 2014*

Name *[es]* *Certificados Reconocidos emitidos por CA ACA Trusted 2014*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *124100380054207126185684841771003655184*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFaTCCBFGgAwIBAgIQXVzdIl2GlqRWFR+LAQm0EDANBgkqhkiG9w0BAQsFADB5MQswCQYDVQQG
EwJFUzE2MDQGA1UEChMtQ29uc2VqbyBHZW5lcmFsIGRlIGxhIEFib2dhY2lhIE5JRjpRLTI4NjMw
MDZJMTIwMAYDVQQDEyIBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTAe
Fw0xNTEwMDcxMzM1MDdaFw0yNTEwMDcxMzM1MDdaMIGqMQswCQYDVQQGEwJFUzEnMCUGA1UECgwe
Q29uc2VqbyBHZW5lcmFsIGRlIGxhIEFib2dhY2lhMTIwMAYDVQQLDCIBdXRvcmlkYWQgZGUgQ2Vy
dGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTESMBAGA1UEBRMJUTI4NjMwMDZJMSowKAYDVQQDDCFB
Q0EgLSBUcnVzdGVkIENlcnRpZmljYXRlcyAtIDIwMTQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC4X2cgVtFvACCdHYMvcfCFFq69s1Aga+obWE/aEYFvZWRzILkGMEQNLb6k6NEuggxfw
FLR1J7w7UQXkgVI6J3kTj6JqCxA3/EO5m83loBYHe9SHIZBZDJm9UQsNZ5QeT+mAnlE9eR6tF3uO
w81JeDZEDgjZ5FVHmsrSuVxqjnmpEQ/B3xcToNal45qAsekzFizsP6XVsEj7lVbrLdCFiVX3RAbi
2iZpTt4AImc4cp5QHystN3vtYVcSagTRkHj2m+BPjOdFGvy5htcnOhdEvb+ANIAnqPkdyTIGr
qr2qDyWlcb4yWMx6dSH+72DUzyvYGaMdtcZvCLxjb3y0lwBHAgMBAAGjggG5MIIBtTA3BgNVHRIE
MDAugRlbYy0tbY2Fib2dhY2lhLm9yZ4YZaHR0cDovL3d3dy5bY2Fib2dhY2lhLm9yZzAPBgNVHRMB
AfBEBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUgY/RYwBKyk0gl6ZSAGAu0sw2i20w
HwYDVR0jBBgwFoAU1lhMjm0EoSCQO/gcmrNnBF95gMYwgasGA1UdIASBozCBoDCBnQYLKwYBBAGB
gRUKAQEwgY0wKQYIKwYBBQUIAgEWHWh0dHA6Ly93d3cuYWNhYm9nYWNpYS5vcmcvZG9jMGAGCCsG
AQUFBwICMFQaUkNvbnN1bHRlIGxhIGRlY2xhcmFjaW9uIGRlIHBy YWNlaWNhcyBkZSBjZXQlaWZp
Y2FjaW9uIGVuIGh0dHA6Ly93d3cuYWNhYm9nYWNpYS5vcmcwaw YDVR0fBGQwYjBgoF6gXIYsaHR0
cDovL3d3dy5bY2Fib2dhY2lhLm9yZy9jcmwvYWNhYm9nYWNpYS5jcmyGLGh0dHA6Ly9jcmwuYWNh
Ym9nYWNpYS5vcmcvY3JsL2FjYWJvZ2FjaWEuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQBq3lISirOQ
ehfyf7UV7Iho/8bAjIc3bsg07nlqgTygzhpvvIU5vpk5XBtOI6VXCdcHIXvR6z6TNKs1IM8z3W6x
qW915FLQDnTkH+i/9g5tDCxdNA//fZTNTCWCM8/7McLBrpTFF79mOMnthTpkMIxfStiDwE8pZf8y
fgX93WpTitEtLXMpLRvYcptC3/P+yVIP2rbYEJ4IW/fYBcy091bU/Es1IwuBntaL3V+v9dByjBcf1
EVd9Jz8o3wKexW02A+XJNoDCZzi6/saX/cO7W1VRmNgLFacGUEgABI5yA8MdguwP8X1Qjt2cgF57
Au3ytfAaEm/grXM9oI+8VTx5eFTB

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion de la Abogacia*

Issuer O: *Consejo General de la Abogacia NIF:Q-2863006I*

Issuer C: *ES*

Subject CN:	*ACA - Trusted Certificates - 2014*
Subject SERIAL NUMBER:	*Q2863006I*
Subject OU:	*Autoridad de Certificacion de la Abogacia*
Subject O:	*Consejo General de la Abogacia*
Subject C:	*ES*
Valid from:	*Wed Oct 07 15:35:07 CEST 2015*
Valid to:	*Tue Oct 07 15:35:07 CEST 2025*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B8:5F:6F:EA:56:D1:6F:00:20:9D:1D:83:2F:72:20:85:16:AE:BD:B3:50:20:6B:EA:21:58:4F:DA:11:81:6F:65:64:6F:20:B9:06:30:44:0D:2D:BE:A4:E8:D1:2E:83:17:F0:14:B4:75:27:BC:3B:51:05:E4:81:52:3A:27:79:13:8F:A2:6A:0B:10:37:FC:43:B9:9B:CD:E5:A0:16:07:7B:D4:87:21:90:59:0C:99:BD:51:0B:0D:67:94:1E:4F:E9:80:9E:51:3D:79:1E:AD:17:7B:8E:C3:CD:49:78:36:44:0E:08:D9:E4:55:47:9A:CA:D2:B9:5C:6A:8E:79:A9:11:0F:C1:DF:17:13:A0:D6:A5:E3:9A:80:B1:E9:33:16:2C:EC:3F:A5:D5:B0:48:FB:95:56:EB:2D:D0:85:89:55:F7:44:06:E2:D9:F6:69:4E:DE:00:22:D9:DC:E1:CA:79:40:7C:AC:B4:DD:EF:B5:56:15:71:26:A0:4D:19:07:8F:69:BE:04:FF:E3:39:D1:46:BF:2E:61:B5:C9:CE:85:D1:2F:6F:E0:0D:94:09:EA:3E:47:72:4E:51:AB:AA:BD:AA:0F:F5:88:71:BE:32:58:CC:7A:75:21:FE:EF:60:D4:CF:2B:D8:19:A3:1D:B5:C6:6F:08:BC:63:6F:7C:B4:97:00:47:02:03:01:00:01*
Issuer Alternative Name	*ac@acabogacia.org*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*81:8F:D1:63:00:4A:CA:4D:20:97:A6:52:00:60:2E:D2:CC:36:8B:6D*
Authority Key Identifier	*FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.16533.10.1.1* *CPS pointer: http://www.acabogacia.org/doc* *CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]*
CRL Distribution Points	*http://www.acabogacia.org/crl/acabogacia.crl* *http://crl.acabogacia.org/crl/acabogacia.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*2C:26:DA:29:72:06:1F:AF:E7:15:13:CD:CD:C3:EB:72:0E:BD:A8:6E:93:AB:04:A1:97:05:99:0C:BA:48:A2:94*

Certificate fields details

Version:	*3*
Serial Number:	*103184541973990179423004459516921083112*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFRzCCBC+gAwIBAgIQTaCesvuQysJTF1k4GA906DANBgkqhkiG9w0BAQUFADB5MQswCQYDVQQG
EwJFUzE2MDQGA1UECbMtQ29uc2VqbyBhZWSlcmFsIGRlIGxhIEFib2dhY2lhIE5lRjpRLTMNjMw
MDZJMTIwMAYDVQQDEytlBdXRvcmlkYWQgZGUgQ2VyaGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTAe
Fw0xNDAzMDUxNzA0NTZaFw0zMDAzMDUxNzA0NTZaMIGqMQswCQYDVQQGEwJFUzEnMCUGA1UECgwe
Q29uc2VqbyBhZWSlcmFsIGRlIGxhIEFib2dhY2lhMTIwMAYDVQQLDCIBdXRvcmlkYWQgZGUgQ2Vy
dGlmaWNhY2lvbiBkZSBsYSBBYm9nYWNpYTESMBAGA1UEBRMJUTI4NjMwMDZJMSowKAYDVQQDDCFB
Q0FgZ.SBUcnVzdGVkIENlcnRpZmlyYXRlcyAtIDIwMTQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC4X2/qVtFvACCdHYMvciCFFq69s1Aga+ohWE/aEYFvZWRvILkGMEQNL b6k6NEugxfw
FLR1J7w7UQXkgVI6J3kTj6lqCxA3/EOSm83loBYH69SHIZBZDJm9UQsNZ5Qe1+mAnlE9eR6tF3uO
w81JcDZEDgjZ5FVHmsrSuVxqimmpEQrB3xc1oNal45qAsekzFizsP6XVsEj7lVbrLdCFiVX3RAbi
2fZpTi4AImc4cpSQHysiN3rlYYcSagTRkHj2m+BPjiQdFGvy5htcnOhdEvb+ANIAnqPkdyTIGr
qr2qD/Wlcb4yWMx6dSH+72DUzyvYGaMdlcZvCLxjb3y0lwBHAgMBAAGjggGXMIIBkzAPBgNVHRMB
AI8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjARBglghkgBhvhCAQEEBAMCAAcwHQYDVR0OBBYEFIGP
0WMASspNIJemUgBgLtLMNottMB8GA1UdIwQYMBaAFPyITI5tBKEgkNP4HJqzZwRfeYDGMIGvBgNV
HSAEgacwgapQwgaEGCysGAQQBgYEVCgEBMIGRMC0GCCsGAQUFBwIBFiFlcmkiaHR0cDovL3d3dy5h
Y2Fib2dhY2lhL.m9yZy9kb2MwYAYIKwYBBQUHAgIwVBpSQ29uc3VsdGUgbGEgZGVjbGFyYWNpb24g
ZGUgcHJlbY3RpY2FzIGRlIGNlcnRpZmlyYWNpb24gZW4gaHR0cDovL3d3dy5hY2Fib2dhY2lhL.m9y
ZzBrBgNVHR8EZDBiMGCgXqBchixodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2NybC9hY2Fib2dh
Y2lhL.mNybHYsaHR0cDovL2NybC5hY2Fib2dhY2lhL.m9yZy9jcmwvYWNhYm9hYWNpYS5jcmwwJQYJ
KoZIhvcNAQEFBQADggEBABEKCbGN8t7tWQ7DDppCSL56RP8BasEP41n465le3yXVj8yyEoBz3djD
cAaZ5SOx+sGMy4e7tDMUeG4RF6gsPtYb/+8v/U2fmEX20vpd8QnxspH4CB2w3MnjhRooz2grn16V
uBFPGpZcJc6uPml9vbR06VPnW52dvwNMarCrbVpGgscvxzIE6uJqZteYY9bRWZdSmX6++A3EUi9T
owyX8C9Ilg9bRmAa7h2f7jbVhhk65JXF/5mvyKl4V7oqJo8mLCvb+XHCKUW5fnUuAqpo1jGm451
02WbNx55PvFiiNf6sWDOYDgfu7U/MYRlryanibPHU7pCd3dmLj6HWDW0dk=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Autoridad de Certificacion de la Abogacia*

Issuer O: *Consejo General de la Abogacia NIF:Q-2863006I*

Issuer C: *ES*

Subject CN: *ACA - Trusted Certificates - 2014*

Subject SERIAL NUMBER: *Q2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia*

Subject C: *ES*

Valid from: *Wed Mar 05 18:04:56 CET 2014*

Valid to: *Tue Mar 05 18:04:56 CET 2030*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B8:5F:6F:EA:56:D1:6F:00:20:9D:1D:83:2F:72:20:85:16:AE:BD:B3:50:20:6B:EA:21:58:4F:DA:11:81:6F:65:64:6F:20
:B9:06:30:44:0D:2D:BE:A4:E8:D1:2E:83:17:F0:14:B4:75:27:BC:3B:51:05:E4:81:52:3A:27:79:13:8F:A2:6A:0B:10:37:FC:43:B9:9B:CD:E5:A0:16:07:7B:D4:87:21:90:59:0C:99:BD:51:0B:0D:67:94:1E:4F:E9:80:9E:51:3D:79:
1E:AD:17:7B:8E:C3:CD:49:78:36:44:0E:08:D9:E4:55:47:9A:CA:D2:B9:5C:6A:8E:79:A9:11:0F:C1:DF:17:13:A0:D6:A5:E3:9A:80:B1:E9:33:16:2C:EC:3F:A5:D5:B0:48:FB:95:56:EB:2D:D0:85:89:55:F7:44:06:E2:D9:F6:69:
4E:DE:00:22:D9:DC:E1:CA:79:40:7C:AC:B4:DD:EF:B5:56:15:71:26:A0:4D:19:07:8F:69:BE:04:FF:E3:39:D1:46:BF:2E:61:B5:C9:CE:85:D1:2F:6F:E0:0D:94:09:EA:3E:47:72:4E:51:AB:AA:BD:AA:0F:F5:88:71:BE:32:58:C
C:7A:75:21:FE:EF:60:D4:CF:2B:D8:19:A3:1D:B5:C6:6F:08:BC:63:6F:7C:B4:97:00:47:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *81:8F:D1:63:00:4A:CA:4D:20:97:A6:52:00:60:2E:D2:CC:36:8B:6D*

Authority Key Identifier *FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*

Certificate Policies

Policy OID: 1.3.6.1.4.1.16533.10.1.1

CPS pointer: uri:http://www.acabogacia.org/doc

CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]

CRL Distribution Points

http://www.acabogacia.org/crl/acabogacia.crl

http://crl.acabogacia.org/crl/acabogacia.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BE:F7:3E:BA:EE:78:9B:5B:7A:FC:E3:87:04:2E:1D:E9:3F:B4:57:BD:3B:A7:DC:CE:5C:BB:9F:A9:9F:15:24:DD*

X509SubjectName

Subject CN: *ACA - Trusted Certificates - 2014*

Subject SERIAL NUMBER: *Q2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-12-04T01:00:00Z

7.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.5.3 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name *[en]* *Qualified Certificates issued by ACA Trusted 2014*

Name *[es]* *Certificados Reconocidos emitidos por CA ACA Trusted 2014*

Service digital identities

X509SubjectName

Subject CN:	*ACA - Trusted Certificates - 2014*
Subject SERIAL NUMBER:	*Q2863006I*
Subject OU:	*Autoridad de Certificacion de la Abogacia*
Subject O:	*Consejo General de la Abogacia*
Subject C:	*ES*

X509SKI

X509 SK I	*gY/RYwBKyk0gl6ZSAGAu0sw2i20=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

7.5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.5.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ACA Trusted 2014*

Name [es] *Certificados Reconocidos emitidos por CA ACA Trusted 2014*

Service digital identities

X509SubjectName

Subject CN: *ACA - Trusted Certificates - 2014*

Subject SERIAL NUMBER: *Q2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia*

Subject C: *ES*

X509SKI

X509 SK I *gY/RYwBKyk0gl6ZSAGAu0sw2i20=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-06-04T22:00:00Z*

7.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.6 - Service (granted): Qualified certificate issued by ACA CA1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificate issued by ACA CA1*

Name *[es]* *Certificados cualificados emitidos por ACA CA1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *97194458065097781445205750873990825389*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHJTCCBQ2gAwIBAgIQSR74wr9HJNNXa9GB/GcFrTANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQG
EwJFUzESMBAGA1UEBRMJUTI4NjMwMDZJMScwJQYDVQQKDB5DT05TRUpPIEdFTkVSQUwgREUgTEEg
QUJPR0FDSUExETAPBgNVBAMMCEFDQSBST09UMB4XDTE2MDYyMzEyMDkzN1oXDTMwMDYyMzEyMDkz
N1owgZYxCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1RMjg2MzAwNkkxMjAwBgNVBAsMKUFV
VE9SSUJRBRCBERSBDRVUSUZQ0IFDSU9OIERFIExBIEFCTOdBQ0IBMSCwJQYDVQQKDB5DT05TRUpP
IEdFTkVSQUwgREUgTEEgQUJPR0FDSUExEDAOBgNVBAMMB0FDQSBDQTEwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQC68P+XTvoGjlVctgPFJEs1fZdo52qa0kioi3qDrDURU4TwH4zywoEE
r/4UQzOzOi7SHCS1LqpEwZmb6lzh18uw4vte/ORrzisSbHIW9148FKesOrr7jyKh+wSniuL6oCED
SnaNcx4+uFvFdZBLwkZ0CG0KoGFpKCY4+MmhNUXlZuTkTqhkGu5Rtiee+sDAa4GJemYt036xUpFNI
E9IZ2TJoSfKNiYN1gcE28lBv4HjYL0AYjyecYsPuEH3SJtElKQOsyL5bDdkDy4jJ31VGdSx135P
88934b3gOGCziN8cTHAjs60kvCOyiNdYEAG8cO9G82n/n1daYQjjwhi/e8SJW3Mwl8TrIdbAu8bu
PByQmThCkKgMkN6aP6csgvBcXoPHUPUQR5+f8ggvVfvVW4w2lS+HH0uy6MSaNXoCFqZv6jA2oyY5
yvVZfm06Cqu4zRouGZHhnWYimMI1/jAzXP8C3VVzaBgKMpAQBLdu1POyO5Y bb2ILKJlmAwOM
TvKsXltVKLbYC3LlbyKMJjdYQxZGap5BKZBty67o9D7rFjK5Fxq9lN4Ko0nMK7Zwt6QdnWaarM9r
zGsVvec9Eo9Ox9Y41VYnld/WHKF86OAxCxn4yIQdqlgL9Ea+8APZoU/nzvPovtXY9YLWt6WYYvBGE
OYHqUOYy+4Ko6mUqcT3HLwIDAQABo4IBpTCCAaEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMD4GA1UdIAQ3MDUwMwYEVR0gADAr
MCkGCCsGAQUFBwIBFh1odHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2RvYzAdBgNVHQ4EFgQUcqnn
1o4CZ6BKTBpnMby3/suEtJswcAYIKwYBBQUHAQEEbDBqMCcGCCsGAQUFBzABhhtodHRwOi8vb2Nz
cC5yZWRhYm9nYWNpYS5vcmcwPwYIKwYBBQUHMAKGM2h0dHA6L y93d3cuYWNhYm9nYWNpYS5vcmcv
Y2VvdGlmaWNhZG0vL2FjYV9yb290LmNydDAfBgNVHSMEGDAWgBQaVcQVMeIxmxHUiHF6AD1wKAW/
zTBIBgNVHR8EXjBcMFqgWKBWhiodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2NybC9hY2FfYXJs
LmNybIYpaHR0cDovL2NybC5hY2Fib2dhY2lhLm9yZy9jcmwvYWNhX2FybC5jcmwwDQYJKoZIhvcN
AQEL BQADggIBAJOBv1EwJMzS9iBTgyO2GOdcl3nZmhuAdXHFeKoqkB0EVn1zcOKDL5SOrVbE25tQ
jUnD8gsgZ6EQ2UI8yJrfs97kYFSvnE9qLkaJAWQKTNkUs6yxaFNQZP+Ztr944pyINp3xLr5NXlGG
M4EIzx6+1MoWwaSFuPI/xn0IPmDWX5nbb7tgoKXntHOEkyr8F5nc3GN2kP9kJc3qcLkmW13eWk
Xafo63mLwXMpjpMBvv6U5sdSCANRHymQ95F5kM7EYs+nbnry+Y3uvqAHu8k1MjDX5baiE5nKc4HO
GcqpUEph3GVMP+mvfTlhCTU9FKQxVrM5ClMC6CPltO7QobgeIdMRX1MUoMnj4nvNLSNR8BgkCIPn
7qxhcbcK631FFkn8Iq4o47dERCNWSmyYZ3H0ohFdKB95OsW45VZFiigTAagcKJlIkdC1wgf4o4kb
kpb16r2P9YuInq+0LcBjQ995U8cWv21FuXZuFjm0NKQSTgDFahoZ+t3XcZmS1iFSXMIP1sLe3c
DMXIlYCtmFZhfXhU09mhP8jnMthPXieH/+kwmkAuOfSDWpEFIti9HJFJ7+wAGgpz1GiOVxZxzTc
4WbuglU+ilgsOZ5koKwsjFIj645E04wjycHrt+H9tPTIm3myOA3WWylWgmeGzHwA3hodqBMkbejN
DUxB89y+Nazp

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ACA ROOT*

Issuer O: *CONSEJO GENERAL DE LA ABOGACIA*

Issuer SERIAL NUMBER: *Q2863006I*

Issuer C: *ES*

Subject CN: *ACA CA1*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject C: *ES*

Valid from: *Thu Jun 23 14:09:37 CEST 2016*

Valid to: *Sun Jun 23 14:09:37 CEST 2030*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BA:F0:FF:97:4E:FA:06:8E:55:5C:B6:03:C5:24:4B:35:7D:97:68:E7:6A:9A:D2:48:A8:8B:7A:83:AC:35:11:53:84:F0:1
F:8C:F2:C2:81:04:AF:F9:78:51:0C:F4:CC:E8:BB:48:70:92:D4:BA:A9:13:06:66:6F:A9:73:87:5F:2E:C3:8B:ED:7B:F3:91:AF:38:92:6C:72:16:F7:5E:3C:14:A7:AC:3A:BA:FB:8F:22:A1:FB:04:A7:8A:E2:FA:A0:21:03:4A:76:8
D:DD:C0:3E:C0:5B:C5:75:90:4B:C0:A6:74:08:62:A8:18:5A:4A:09:8E:3E:32:68:4D:51:7D:19:B9:39:13:AA:19:06:BB:94:6D:89:E7:BE:B0:30:1A:E0:62:5E:9A:26:34:DF:AC:54:A4:53:48:13:D2:19:D9:32:68:49:F2:8D:89:83:
75:81:C1:36:F2:50:6F:E0:78:D8:2F:40:18:8F:27:9C:62:C3:EE:10:77:C9:48:98:84:94:A4:0E:B3:22:F9:6C:37:64:0F:2E:23:27:7D:55:19:D4:B1:D7:7E:4F:F3:CF:77:E1:BD:E0:38:60:B3:88:DF:1E:4C:70:23:B3:AD:24:BC:23:B
2:88:D7:58:10:01:BC:70:EF:46:F3:69:FF:9F:57:5A:61:08:E3:C2:18:BF:7B:C4:89:5B:73:30:97:C4:EB:21:D6:C0:BB:C6:EE:3C:1C:90:99:38:42:90:A8:0C:90:DE:9A:3F:A7:2C:82:F0:5C:5E:83:C7:50:F5:10:47:9F:9F:F2:08:2F
:55:FB:D5:5B:8C:36:21:2F:87:1F:4B:B2:E8:C4:9A:35:7A:02:16:A6:6F:EA:30:36:A3:26:39:CA:F5:59:21:F9:90:E8:28:EA:BB:8C:D1:A2:28:86:64:78:67:59:87:E6:30:8D:7F:8C:0C:D7:3F:D0:B7:55:5A:DA:06:A2:8C:A4:04:0
1:2D:DB:B5:3C:EC:8E:E5:86:DB:D8:82:CA:26:59:80:8B:03:8C:4E:F2:AC:5E:5B:55:28:B6:D8:0B:72:E5:87:22:8C:26:37:58:43:16:46:6A:9D:C1:29:90:6D:CB:AE:E8:F4:3E:EB:16:32:B9:17:1A:BD:94:DE:0A:A3:49:CC:2B:
B6:70:8B:A4:1D:9D:66:9A:AC:CF:6B:CC:6B:15:BD:E7:3D:12:8F:4E:C7:D6:38:D5:56:27:95:DF:D6:1C:A1:7C:E8:E0:31:0B:19:F8:C8:84:1D:AA:58:0B:F4:46:BE:F0:03:D9:A1:49:F3:BC:FA:2F:B5:76:3D:60:B5:AD:E9:66:
18:BC:11:84:39:81:EA:50:E6:32:FB:82:A8:EA:65:2A:71:3D:C7:2F:02:03:01:00:01
```

Basic Constraints	*IsCA: true*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.acabogacia.org/doc*
Subject Key Identifier	*72:A9:E7:D6:8E:02:67:A0:4A:4C:1A:67:31:BC:B7:FE:CB:84:B4:9B*
Authority Info Access	*http://ocsp.redabogacia.org* *http://www.acabogacia.org/certificados/aca_root.crt*
Authority Key Identifier	*1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD*
CRL Distribution Points	*http://www.acabogacia.org/crl/aca_arl.crl* *http://crl.acabogacia.org/crl/aca_arl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*70:5E:B3:A0:B1:F0:9D:ED:A3:ED:45:76:6B:BB:C0:21:97:70:0A:BB:1E:2D:1D:9E:28:62:AC:58:9D:C9:FD:77*

X509SubjectName

Subject CN:	*ACA CA1*
Subject O:	*CONSEJO GENERAL DE LA ABOGACIA*
Subject OU:	*AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*
Subject 2.5.4.97:	*VATES-Q2863006I*
Subject C:	*ES*

X509SKI

X509 SK I	*cqnn1o4CZ6BKTBpnMby3/suEtJs=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-11-02T00:00:00Z

7.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.7 - Service (granted): Qualified certificates issued by ACA CA2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by ACA CA2*
Name	*[es]*	*Certificados cualificados emitidos por ACA CA2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *97911743187377240900748830157217551837*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHJTCCBQ2gAwIBAgIQSakdpc0NcMNXa9EcAJ1V3TANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQG
EwJFUzESMBAGA1UEBRMJUT4NjMwMDZJMScwJQYDVQQKDB5DT05TRUpPIEdFTkVSQUwgREUgTEEg
QUJPR0FDSUExETAPBgNVBAMMCEFDQSBST09UMB4XDTE2MDYyMzEyMDc1OFoXDTMwMDYyMzEyMDc1
OFowgZYxCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1RMjg2MzAwNkkxMjAwBgNVBAsMKUFV
VE9SUlRBRCBERSBDRVJUSUZJQ0FDSUl9OIERFIExBIEFCT0dBQ0IBMSCwJQYDVQQKDB5DT05TRUpP
IEdFTkVSQUwgREUgTEEgQUJPR0FDSUExEDAOBgNVBAMMB0FDQSBDQTIwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDqfG9fqSYMaxpOxEWQgfNOMFfc0PAbc43C2At5AzKCremMqmPoQncp
pcdXZ7pyWzG6Nl9I9e4u+Qxi8/DKSW3sukUQsMbdgB5Y7MYHUecjpnxgwxToxSN9nDM3WgYUEsj/
dVHhlNg1tjwWNQBSYmz/0pT/V19dhF1uHTr7FgRhjD6sJvx7EnpM1Btxj0e51UwrNT04Kk8FBEG0
tEEgOtULHgtMnA6hLqN1kCkxZru0Guba6YRUxet8zgzDuUuXrL6uE+4weluQKzS5hgvyVhQh+VF
XtKwTADwUzghn188f/tpCbOdlOjSSZ3NWx9bFYcEsaQcDdATxHxJptSJikePCVQYkGEgAuFWs4F
taDfa05FHECE4YkjA2nereGc89OgrYg8B/ypUorSQxmqDfrrqqxZkyOCVMhxzD152M/5cCB6AY1
QemMPKjFWkiGKotWdz50x0VLTXKTCc8eRcflIr4QNEW//wkduOKsSFTJUNpYfMxiRYaXwiJFOG+N
YLTUxEs8w1c6VF1jZGR7FfhebiHR2DDmusuUncgRHh5eqtvHT9FhUtWWr4f5PtFTyyMXzjIIbeBI
xoAtaBhnOeB4SFDYyWWOL7aq4HrQW+KufsoMRKauXwFxCO7CunTI2bQPLUpoNyraxkTQT28IPRa1
bn9TQhmSNcX2l3luZv9jEwIDAQABo4IBpTCCAaEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMD4GA1UdIAQ3MDUwMwYEVR0gADAr
MCkGCCsGAQUFBwIBFh1odHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2RvYzAdBgNVHQ4EFgQUihUf
r3TvHwEHcyqQKkEJftIl0MAweAYIKwYBBQUHAQEEbDBqMCcGCCsGAQUFBzABhhtodHRwOi8vb2Nz
cC5yZWRhYm9nYWNpYS5vcmcwPwYIKwYBBQUHMAKGM2h0dHA6L y93d3czaYWNhYm9nYWNpYS5vcmcv
Y2VydGlmaWNhZG9zL2FjYV9yb290LmNydDAfBgNVHSMEGDAWgBQaVeQVMeIxmxHUiHF6AD1wKAW/
zTBlBgNVHR8EXjBcMFqgWKBWhilodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2NybC9bY2FfYXJs
LmNybIYpaHR0cDovL2NybC5bY2Fib2dhY2lhLm9yZy9jcmwvYWNhX2FybC5jcmwwDQYJKoZIhvcN
AQELBQADggIBALP7TopBAMAXQtbjtvbyZ213WvYdN+ECdIjWjb2l/uKRbeAovwldEMauVmnF1W40
dsxYhsb5TMZRaCeo6P2ZWYoQ2ny41iqguMGAof647ExHLtG+TanqzZE6wiiuz3PSwTgHjKpmsFgh
MCaHMldMo44Ncn9ZqKKgozi VW8vRzlEQUBeC/z0tylRd4tWmm33EXlLsDLbKa+85Rei9+FeRdF3t
FtA5Cx3ih1ASjGejPISBXq29xyB5bQ3E2TmMXMFtEu/txFHivkvytsye1bLWQLHP7FiwrwPm2DD
AGwkFvXv+IBt/xUbyGjK9vXy745Nn0ffhzfc49IxmMNbt0R0vsM/koWQ8wzjQQw2RUjjGM
jqxamd+RXyL52kzoTXOBsjDrbtFQSDJh5BUCt8nkEZBxhtmPeMxY1Gpyotjo2mhXzchp9jH0LpLk
ag80A6nDZUmotxD5u4wrg3gFEgm7ZCWxhrvyh8oMVDdH1FDsGz3bRPlggh8ZO8jtPlVco4r3Dnjb
emjQzZlXaZdXYFRlDLRuWWgpXoyO++MKexKm8bLU4s9ZjgOy2t9h6aaXmPWZAwIfQaO9luwleZuy
5p/AA8rvZ1g7PeSCXKmM5ISuG/6/0Eu8VWLQ2sMd2rKE6Cz1PoObW1mq91CYx6QUZUsE97CqCM
nHx+M1KBWtJY

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ACA ROOT*

Issuer O: *CONSEJO GENERAL DE LA ABOGACIA*

Issuer SERIAL NUMBER: *Q2863006I*

Issuer C: *ES*

Subject CN: *ACA CA2*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject C: *ES*

Valid from: *Thu Jun 23 14:07:58 CEST 2016*

Valid to: *Sun Jun 23 14:07:58 CEST 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EA:14:6F:48:A9:26:0C:6B:1A:4E:C4:45:90:A8:F3:4E:30:57:DC:D0:F0:1B:73:8D:C2:D8:0B:77:03:32:82:AD:E9:8C:AA:63:E8:42:77:A9:A5:C7:57:67:BA:72:5B:31:BA:34:8F:48:F5:EE:2E:F9:0C:62:F3:F0:CA:49:6D:EC:BA:45:10:B0:C6:DD:80:1E:58:EC:C6:07:51:E7:23:A6:7C:60:C3:14:E8:C5:23:7D:9C:33:37:5A:06:14:12:C8:FF:75:51:E1:20:D8:08:B6:3C:16:35:00:52:62:6C:FF:D2:94:FF:57:5F:5D:84:5D:6E:1D:3A:FB:16:04:61:8C:3E:AC:26:FC:7B:12:7A:4C:D4:1B:71:8F:47:B9:21:4C:1F:35:3D:38:2A:4F:05:04:41:B4:B4:41:20:3A:DF:CB:1E:0B:4C:9C:0E:A1:2E:A3:75:90:29:31:67:3B:B4:1A:E6:DA:E9:84:54:C5:EB:7C:CE:0C:C3:B9:4B:6E:5E:B2:FA:B8:4F:B8:C1:E9:6E:40:AC:F9:4A:18:2F:C9:58:50:87:E5:45:5E:42:B0:4C:00:F0:53:38:21:9F:5F:3C:7F:FB:69:09:B3:9D:94:E8:D2:49:9D:CD:5B:1F:61:15:57:84:B1:A4:1C:0D:D0:13:C4:7C:49:A5:F4:89:8A:47:8F:09:54:18:28:61:2A:8C:0B:85:5A:CE:05:B5:A0:DF:6B:4E:45:1C:40:84:E1:89:23:03:69:DE:AD:E1:9C:F0:6F:74:82:B6:20:F0:1F:F2:A5:4A:2B:49:0C:66:A8:37:EB:AE:AA:B1:66:4C:8E:09:53:21:C7:30:F5:E7:63:3F:E5:C0:81:E8:06:22:41:E9:8C:3C:A8:C5:5A:48:86:2A:87:D6:77:3E:74:C7:45:4B:4D:72:93:09:CF:1E:45:C7:E5:22:BE:10:34:45:BF:FF:09:1D:B8:E2:AC:48:54:C9:50:DA:58:7C:CC:62:45:86:97:C2:22:45:38:6F:8D:60:B4:D4:C4:4B:3C:C3:57:3A:54:5D:63:64:64:7B:15:F8:5E:6E:21:D1:D8:30:E6:BA:CB:94:9D:C8:11:1E:1E:5E:AA:DB:C7:4F:D1:61:52:D5:96:AF:87:F9:3E:D1:53:8B:23:17:CE:37:ED:6D:E0:65:C6:80:21:68:16:E7:39:E0:78:48:50:D8:C9:65:8E:2F:BB:AA:E0:7A:D0:5B:E2:AE:22:CA:0C:44:A6:AE:5F:01:71:08:EE:C2:BA:74:C8:D9:B4:0F:2D:4A:68:37:2A:DA:C6:44:D0:4F:6F:25:3D:16:B5:6E:7F:53:42:19:92:35:E5:F6:97:79:6E:66:FF:63:13:02:03:01:00:01

Basic Constraints *IsCA: true*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.acabogacia.org/doc

Subject Key Identifier *8A:15:1F:AF:74:EF:1F:01:07:73:2A:90:2A:41:09:7E:1B:48:D0:C0*

Authority Info Access

http://ocsp.redabogacia.org

http://www.acabogacia.org/certificados/aca_root.crt

Authority Key Identifier *1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD*

CRL Distribution Points

http://www.acabogacia.org/crl/aca_arl.crl

http://crl.acabogacia.org/crl/aca_arl.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7E:93:16:A5:CE:CF:B9:0A:53:AD:C3:C7:76:94:50:F4:2C:DC:3A:9B:85:DF:4C:75:77:B0:53:DC:BB:25:58:12*

X509SubjectName

Subject CN: *ACA CA2*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject C: *ES*

X509SKI

X509 SK I *ihUfr3TvHwEHcyqQKkEJfhtI0MA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-12-04T01:00:00Z*

7.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

7.7.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by ACA CA2*

Name *[es]* *Certificados cualificados emitidos por ACA CA2*

Service digital identities

X509SubjectName

Subject CN: *ACA CA2*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject C: *ES*

X509SKI

X509 SK I *ihUfr3TvHwEHcyqQKkEJfhtI0MA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-11-02T00:00:00Z*

7.7.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.8 - Service (granted): Qualified certificates issued by ACA CA3

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by ACA CA3*

Name *[es]* *Certificados cualificados emitidos por ACA CA3*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *114392107427724248384195985487754308843*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHJTCCBQ2gAwIBAgIQVg8eVqYwsNRXa8/pD7os6zANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQG
EwJFUzESMBAGA1UEBRMJUTI4NjMwMDZJMScwJQYDVQQKDB5DT05TRUpPIEdFTkVSQUwgREUgTEEg
QUJPR0FDSUExETAPBgNVBAMMCEFDQSBST09UMB4XDTE2MDYyMzEyMDI0OVoXDTMwMDYyMzEyMDI0
OVowgZYxCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1RMjg2MzAwNkkxMjAwBgNVBAsMKUFV
VE9SSURBRCBERSBDRVJUSUZJQ0FDSU9OIERFIEsBIEFCT0dB0ilBMScwJQYDVQQKDB5DT05TRUpP
IEdFTkVSQUwgREUgTEEgQUJPR0FDSUExEDAOBgNVBAMMB0FDQSBDQTMwggIhMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDCiKMFfK6sNsbdt9NpYmYiVxsajASI+Q+8Bveq9wUimrgR+9HPg9Xi
fShCutwksSBilcV+AUplbbDYmYc7x1XThBqu0/Of2dEkPcJWI0h6LIh99Uaw90aKGQSeCr3iBwQD
ygAZk7gJMRyCc7DQ0qvy8cByePDuzkfdUhMrFAhr/a9dP0dr//Gy4/jCWQ+MM7TQ3DZIVdgyLO6
kPzJWvajzIJBzu/kj6p+DU89EGfa8zNk3v82dVc53cx8Ysys8rq5WzkOXHY0pndLOCbvpnBapLZ
5fhKt/J4z9YD2EbBJ9P0xyK5+GUKEuEXCDJgCIMcRncdPqtA/udsM1BlBHIpolbUOVWlccSZ7tl
grVi6e8bgA5RbBH0drFADcXOfyg0bTZt00MOPgA42LePrQYgl9D/1kbSsS366QbEyplh0Ul8lGHf
6gMK5z2TxcD71tSNtRkxAHe3uKEhSedUVfBrv3yIiXaZIlCMx2X3vDoGqVW2BgIuFkb5Ul/lVlbcJ
69OD13CaUoPmsdZNgKQdUg9sTmJnNGz5hvarfcxMB7h47M+tLA2dLSWFCosdY5yxQprTLAG08NC1k
4N+BbXD4cZ9xJmFvAxPAr4tvatb6FHA1jnUHZQ+O4H1dDU21WHdaVRLDIDPSrorHWAAXQ1L11TfQ
aq3HXuYTCTnFZUgpaekHYwIDAQABo4IBpTCCAaEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMD4GA1UdIAQ3MDUwMwYEVR0gADAr
MCkGCCsGAQUFBwIBFh1odHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2RvYzAdBgNVHQ4EFgQUPfjd
AbrGKMVMtJnC8K3mIzWVTy8weAYIKwYBBQUHAQEEbDBqMCcGCCsGAQUFBzABhhtodHRwOi8vb2Nz
cC5yZWRhYm9nYWNpYS5vcmcwPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYWNhYm9nYWNpYS5vcmcv
Y2VydGlmaWNhZG9zL2FjYV9yb290LmNydDAfBgNVHSMEGDAWgBQaVeQVMeIxmxHUiHF6AD1wKAW/
zTBlBgNVHR8EXjBcMFqgWKBWhlodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2NybC9hY2FfYXls
LmNybI1paHR0cDovL2NybC5hY2FjbzdhY2lhLmy9zZy9jcmwvYWNhX2FybCBjcmwvDQYJKoZIhvcN
AQELBQADggIBAJjuRnOjmgbDRE7V3bfC7KNfA6J8Wkf3PyqgVwrSmU/af6YVRP+/XdoOGrvf4ILR6
LRCGzZERcjoQa4X1IPqdHa8PnSzku3Ag8XNyGllVlg8iTPA4Vm5YcdpJGRBS5+KObRG34KMMBghm
WRRJU/C+yMNk/35e9e1JcZ4NjsNTs1jmBcV6xzmpNZt0lti84i7Ogo0CJOnJC3wH46two9L0kQFM68
WXtGgQgSAcwkbKpSHCcOdrNjTucWzp0uHkpgAMLKnJ0c6kgZBR7k7wByP4ItgHYgFaWfXCit9a/c
CVRJqwS1ygSajp77YVsxj4fPu1ONsfhCF6FermNCktJeOYWstsbStZlGW+Oq2nC9p/ZdVbtF9D
6CLYhbMZx4G+6ixFletyqrpldFUIrghtcP6M6DCYXW6tGDil0I1PmIdxWxypPtdQWFydxGbgaffx
xGL9ku/IGLs3T3zLmPuXwRb+TRr1axIhyVDVsnO6Ozclh8RbLHFpYsNde7emdg86HdFaE010ta
pYjrbeC/mEw7dtcOyTTgnkZagaV1nWvX2KcChotyin2GLNL6iM4ewkQAUlQvQzmOIF4k3g8bjbCE
PoPMw/Uis4Ya76+yKlooX4fdl0AcVdDvz5fvJJyv6oTCAEeLdDcqZnrAiYo/0x+RGJHpj/sSUv03
I6eDl0LRGKJL
-----END CERTIFICATE-----
```

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ACA ROOT*
Issuer O:	*CONSEJO GENERAL DE LA ABOGACIA*
Issuer SERIAL NUMBER:	*Q2863006I*
Issuer C:	*ES*
Subject CN:	*ACA CA3*
Subject O:	*CONSEJO GENERAL DE LA ABOGACIA*
Subject OU:	*AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*
Subject 2.5.4.97:	*VATES-Q2863006I*
Subject C:	*ES*
Valid from:	*Thu Jun 23 14:02:49 CEST 2016*
Valid to:	*Sun Jun 23 14:02:49 CEST 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C2:88:A3:05:7C:AE:AC:36:C6:DD:B7:D3:69:62:66:22:57:1B:1A:8C:04:88:F9:0F:BC:06:F7:AA:F7:05:26:AF:F8:11:FB:D1:CF:83:D5:E2:7D:28:42:BA:DC:24:B1:20:62:95:C5:7E:01:4A:65:6D:B0:D8:99:87:3B:C4:85:D3:84:1A:AE:D3:F3:9F:D9:D1:24:3D:C2:56:23:48:7A:2E:58:7D:F5:46:B0:F7:46:8A:19:04:9E:0A:BD:ED:07:04:03:CA:00:19:93:B8:09:31:1C:82:73:B0:DD:D2:AB:F2:F1:C0:72:78:F0:EE:CE:47:E2:75:48:4C:AC:50:21:AF:F6:BD:74:FD:1D:AF:FF:C6:CB:8F:E3:09:64:3E:30:CE:D3:43:70:D9:21:57:60:CS:B3:BA:90:FC:C9:5A:F6:A3:8F:32:09:07:3B:BF:92:3E:A9:F8:35:3C:F4:41:9F:6B:CC:4D:93:7B:FC:D9:D5:5C:E7:77:31:F1:8B:6C:CB:CA:EA:E5:6C:E4:3B:F5:C7:63:4A:6C:74:B3:82:6E:FA:7C:6A:92:F6:E5:F8:4A:B7:F2:78:CF:D6:03:D8:46:C1:27:D3:F4:C7:22:B9:F8:65:0A:12:E1:17:08:3B:49:80:27:CC:71:19:DC:74:FA:AD:03:FB:9D:B0:CD:41:94:17:C7:A6:89:5B:50:E5:56:95:C7:39:67:BB:65:82:B5:62:E9:EF:1B:80:0E:51:6C:11:F4:76:B1:40:0D:E5:CE:7F:28:34:6D:36:6D:D3:43:0E:3E:00:38:D8:B7:8F:AD:06:20:97:D0:FF:97:59:1B:4A:C4:B7:EB:A4:1B:13:2A:48:87:45:3C:94:61:DF:EA:03:0A:E7:3D:93:C5:C0:FB:D6:D4:8D:B5:19:31:00:77:B7:B8:A1:21:49:E7:54:55:F0:6B:BF:7C:B5:89:76:99:22:50:8C:C7:65:F7:BC:3A:06:A9:55:B6:06:07:EE:16:46:F9:52:58:95:95:B7:09:EB:D3:83:D7:70:9A:0E:83:E6:B3:86:4D:80:A4:38:52:0F:6C:4E:6D:E7:34:6C:F9:86:F6:AB:EB:13:01:EE:1E:3B:33:EB:4B:03:67:4B:49:61:42:A2:C2:58:E7:2C:50:A5:F4:CB:00:6D:3C:34:2D:64:E0:DF:81:6D:70:F8:79:9F:71:26:61:6F:03:13:C0:AF:8B:6F:6A:D6:FA:14:70:35:8E:75:07:65:0F:8E:E0:7D:5D:0D:4D:B5:58:77:5A:55:12:C3:94:33:D2:AE:8A:C7:58:00:17:43:52:F5:D5:37:D0:6A:AD:C7:5E:E6:13:09:39:C5:65:48:29:69:E9:07:63:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Extended Key Usage	*id_kp_serverAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.acabogacia.org/doc*
Subject Key Identifier	*3D:D8:DD:01:BA:C6:28:C5:4C:B5:39:C2:F0:AD:E6:D7:35:95:4F:2F*
Authority Info Access	*http://ocsp.redabogacia.org* *http://www.acabogacia.org/certificados/aca_root.crt*
Authority Key Identifier	*1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD*
CRL Distribution Points	*http://www.acabogacia.org/crl/aca_arl.crl* *http://crl.acabogacia.org/crl/aca_arl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *AF:57:FD:80:5A:0E:F9:0E:97:57:65:C0:D5:D5:5E:3F:D2:4C:FC:49:B7:3A:A1:A4:9E:19:79:01:8D:54:FC:26*

X509SubjectName

Subject CN: *ACA CA3*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject C: *ES*

X509SKI

X509 SK I *PdjdAbrGKMVMtTnC8K3m1zWVTy8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-12-04T01:00:00Z

7.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

8 - TSP: Colegio de Ingenieros de Caminos, Canales y Puertos

.

TSP Name

Name	*[en]*	*Colegio de Ingenieros de Caminos, Canales y Puertos*
Name	*[es]*	*Colegio de Ingenieros de Caminos, Canales y Puertos*

TSP Trade Name

Name	*[en]*	*CICCP*
Name	*[es]*	*CICCP*
Name	*[en]*	*VATES-Q2867009I*
Name	*[en]*	*CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

PostalAddress

Street Address	*[es]*	*Almagro, 42*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28010*
Country Name	*[es]*	*ES*

PostalAddress

Street Address	*[en]*	*Almagro, 42*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28010*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:informatica@ciccp.es*
URI	*[en]*	*http://www.ciccp.es*

TSP Information URI

URI	*[en]*	*http://www.ciccp.es*
URI	*[es]*	*http://www.ciccp.es*

8.1 - Service (withdrawn): Qualified Certificate

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificate*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA CICCP Clase 3 PKI anterior*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *458165872953085692739587*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGITCCBQmgAwIBAgIKYQU4xAAAAAAAAzANBgkqhkiG9w0BAQUFADCBxzELMAkGA1UEBhMCRVMx
DzANBgNVBAgTBk1hZHJpZDEPMA0GA1UEBxMGTWFkcmlkMUMwQQYDVQQKEzpDSUNDUCAtIENvbGVn
aW8gZGUgSW5nZW5pZXJvcyBkZSBDYW1pbm9zIENhbmFsZXMgeSBQdWVvdG9zMSEwHwYDVQQLExhD
SUNDUCBDLkkuRs4gU0yODY3MDA5LUlcETAPBgNVBAMTCENBIEJQ0NQMRswGQYJKoZIhvcNAQkB
Fgxwa2lAY2lj Y3AuZXMwHhcNMDIxMDIzMTUxNjM0WhcNMDYwMTIzMTUyNjM0WjCBzzEbMBkGCSqG
SIb3DQEJARYMcGtpQGNpY2NwLmVzMQswCQYDVQQGEwJFUzEPMA0GA1UECBMGTWFkcmlkMQ8wDQYD
VQQHEwZNYWRyaWQxQzBBBgNVBAoTOkNJQ0NQICOgQ29sZWdpbyBkZSBJbmdlbmllcm9zIGRlIENh
bWlub3MgQ2FuYWxlcyBSIFB1ZX00b3MxITAfBgNVBAsTGENJQ0NQIEMuSS5GLiBRLT14NjcwMDkt
STEZMBcGA1UEAxMQQ0EgQ0IDQ1AgQ2xhc2Ugc2MzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBALk96x16kiGLvv1Imbihmi40mCEV3JkLcslDxJqn3CTdaCdBogPeuVhk1IQV7nL5COSqCpD4
WLqic4BEm7AqWvcAWkp/mZB7mhw5bfpdY0tnNY2oH0ubsUWgnQOTu6fi7C7hEQEE7kA5l8ltkJoH
vlhaK3swGosKq6bcc4mQg5nxFJiGhylkAt6P1hlI0PpjpYJwSi3XrGPQHyysCrAuyIA/PgHCcGMGA
SPAgeYR2xFNaCcR1JyS5zCOZOoeW4FCqlRB0BxcHZrB0/I288ZsS8iKHyLXRcVBZqS9QQrNuB5F9
TQlqk3ageFZdPlNsNStGvB95ALXysdG/MLy/2TxjgusCAwEAAaOCAgMwggH/MBAGCSsGAQQBgjcV
AQQDAgEAMB0GA1UdDgQWBBTujkNO3FP3bSQBPRxERjYIB6K7+zALBgNVHQ8EBAMCAcYwDwYDVR0T
AQH/BAUwAwEB/zCB0gYDVR0jBIHKMIHHgBS63et/HVUS0R+wFzmCBtaZrOwqGBqaSBpjCBozEL
MAkGA1UEBhMCRVMxEjAQBgNVBAgTCUlBUkNFTE9QQTESMBAGA1UEBxMJQkFSQ0VMT05BMRkwFwYD
VQQKExBJUFMgU2VndXJpZGFkIENBMRgwFgYDVQQLEw9DZXJ0aWZpY2FjaW9uZXMxFzAVBgNVBAMT
DkQiUyBTRVJWSURPUkVTMR4wHAYJKoZIhvcNAQkBFg9pcHNAbWFpbC5pcHMuZXOCAwCQGjBjBgNV
HR8EXDBaMCmgJ6AlhiNodHRwOi8vcGtpLmNpY2NwLmVzL3BraS9jYWNpY2NwLmNybDAtoCugKYYn
aHR0cDovL3BraWJhY2uuY2ljY3AuZXMvcGtpL2NbY2ljY3AuY3JsMHQGCCsGAQUFBwEBBGgwZjAv
BggrBgEFBQcwAoYjaHR0cDovL3BraS5jaWNjcC5lcy9wa2kvY2FjaWNjcC5jcnQwMwYIKwYBBQUH
MAKGJ2h0dHA6Ly9wa2liYWNrLmNpY2NwLmVzL3BraS9jYWNpY2NwLmNydDANBgkqhkiG9w0BAQUF
AAOCAQEAnAaRlcF9M/LIJL0YdRqkg9KIcIx3Ss1tO8voZ+HJugauLSkTNs+gVReC4bbnlwa0u9l
zpqBRt9w/k9AEqnDHsgSWNFSPbyD7j25M+Y/j+FZaY3TVPxUNYDLZ4SFIoWF/Ms7kMvJs3b9FTY
ZPAOPyO6JKgXXnCD/xNOw6HTzHUEhp0fSCQ73+b4sriwbl7rcGTxp2Um+4RdUKRU9tTIp1bcA0Y
swRU8rSpxe1iPKRMZcOBjZ6B+WKZVMY46V6DeL5Qa6qXDo5WE8EsYDV+0Ns5Va/HH6/OF9WJtuJ
fAHxCSQ+tqsUoa+GJR91I2xDreUDlnXZO1YIqZoceITmOQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer E: *pki@ciccp.es*

Issuer CN: *CA CICCP*

Issuer OU: *CICCP C.I.F. Q-2867009-I*

Issuer O: *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Issuer L: *Madrid*

Issuer ST: *Madrid*

Issuer C:	*ES*
Subject CN:	*CA CICCP Clase 3*
Subject OU:	*CICCP C.I.F. Q-2867009-I*
Subject O:	*CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*
Subject L:	*Madrid*
Subject ST:	*Madrid*
Subject C:	*ES*
Subject E:	*pki@ciccp.es*
Valid from:	*Wed Oct 23 17:16:34 CEST 2002*
Valid to:	*Mon Jan 23 16:26:34 CET 2006*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:3D:EB:1D:7A:92:21:8B:BE:FD:48:99:B8:A1:9A:2E:34:98:21:15:DC:99:0B:7A:C9:43:C4:9A:A7:DC:24:DD:68:27:41:A2:03:DE:B9:58:64:D6:54:15:EE:72:F9:08:E4:AA:0A:90:F8:58:BA:A2:7B:80:44:9B:B0:2A:5A:F7:00:5A:4A:7F:99:90:7B:9A:1C:39:6D:FA:5D:63:4B:67:35:8D:A8:1F:4B:9B:B1:45:A0:9D:03:93:BB:A7:E2:EC:2E:E1:11:01:04:EE:40:39:97:C2:2D:90:9A:07:BE:58:5A:2B:7B:30:1A:8B:3C:AB:A6:DE:73:89:90:83:99:F1:14:98:86:87:29:64:03:A3:F5:86:52:34:3E:98:E9:60:9C:12:8B:75:EB:18:F4:07:CB:2B:02:AC:0B:B2:20:0F:CF:80:70:9C:18:C1:80:E4:F0:20:CD:84:76:C4:53:5A:09:C4:53:27:24:B9:CC:23:99:3A:87:96:E0:50:AA:95:10:4E:07:17:07:66:B0:74:FC:8D:BC:F1:9B:39:4B:42:87:C8:B5:D1:79:5F:19:8D:2F:50:42:B3:6E:07:91:7D:4D:09:6A:93:76:A0:78:56:5D:3C:83:6C:35:2B:46:BC:1F:79:00:B5:F2:B1:D1:BF:30:BC:BF:D9:3C:63:82:EB:02:03:01:00:01*
Subject Key Identifier	*EE:8E:43:4E:DC:53:F7:6D:24:01:3D:1C:44:46:36:1F:07:A2:BB:FB*
Basic Constraints	*IsCA: true*
Authority Key Identifier	*BA:DD:EB:7F:1D:55:12:D1:1F:B0:17:39:82:7C:1B:5A:66:B3:B0:8A*
CRL Distribution Points	*http://pki.ciccp.es/pki/caciccp.crl* *http://pkiback.ciccp.es/pki/caciccp.crl*
Authority Info Access	*http://pki.ciccp.es/pki/caciccp.crt* *http://pkiback.ciccp.es/pki/caciccp.crt*
Key Usage:	*digitalSignature - nonRepudiation - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*DD:5A:AB:55:AB:2D:22:CC:CB:DB:C3:71:33:CC:FB:B3:E5:1A:D4:B9:C3:3C:EC:15:3F:AF:3B:48:B6:8C:58:C2*

X509SubjectName

Subject CN:	*CA CICCP Clase 3*
Subject OU:	*CICCP C.I.F. Q-2867009-I*
Subject O:	*CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

8.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.1.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificate*

Name *[es]* *Certificados Reconocidos emitidos por la CA CICCP Clase 3 PKI anterior*

Service digital identities

X509SubjectName

Subject CN: *CA CICCP Clase 3*

Subject OU: *CICCP C.I.F. Q-2867009-I*

Subject O: *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

X509SKI

X509 SK I	*7o5DTtxT920kAT0cREY2Hweiu/s=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*
Status Starting Time	*2010-01-25T00:00:00Z*

8.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificate*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA CICCP Clase 3 PKI anterior*

Service digital identities

X509SubjectName

Subject CN:	*CA CICCP Clase 3*
Subject OU:	*CICCP C.I.F. Q-2867009-I*
Subject O:	*CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*
Subject L:	*Madrid*
Subject ST:	*Madrid*
Subject C:	*ES*
Subject E:	*pki@ciccp.es*

X509SKI

X509 SK I	*7o5DTtxT920kAT0cREY2Hweiu/s=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2005-03-03T00:00:00Z*

8.2 - Service (withdrawn): Qualified Certificate

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificate*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA CA CICCP Clase 3*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *135031685893278259059350935028450579902*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGczCCBGOgAwIBAgIQZZYoH3oF77FCwRIZu/XVvjANBgkqhkiG9w0BAQUFADCBzzEbMBkGCSqG
SIb3DQEJARYMcGtpQGNpY2NwLmVzMQswCQYDVQQGEwJFUzEPMA0GA1UECBMGTWFkcmlkMQ8wDQYD
VQQHEwZNYWRyaWQxQzBBBgNVBAoTOkNJQ0NQIC0gQ29sZWdpbyBkZSBJbmdlbmllcm9zIGRlIlENh
bWlub3MgQ2FuYWxlcyBSIFB1ZX0b3MxITAfBgNVBAs1TGENJQ0NQIEMuSS5G1JiBRL1T4NjcwMDkt
STEZMBcGA1UEAxMQQ0EgQ0IDQ1AgQ2xhc2Ig MzAcFwtwOTA4MTcxMDI1MjthaFwtxOTA4MTcxMDM1
MjZaMIHPMRswGQYJKoZIhvcNAQkBFgxwa2lA Y2ljY3AuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQI
EwZNYWRyaWQxDzANBgNVBAcTBk1hZHJpZDFDMEEGA1UEChM6Q0lDQ1AgLSBDb2xlZ2lvIGRlIElu
Z2VuaWVyb3MgZGUgQ2FtaW5vcyBDYW5hbGVzIHkgUHVlcnRvczEhMB8GA1UECxMYQ0lDQ1AgQy5J
LkYuIFEtMjg2NzAwOS1JMRkwFwYDVQQDExRDQSBDSUNDUCBDbGFzZSAzMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEA0HLO+zAhSicUThx40eycdWgH90CC24XhgbKR354dRoQ+qrg+NgJt
gW2oHJ2xvkEQWHFseLe7Y3GlkWUUp6Xc++9YfaGr1SLkkMFf5nh0GAvDuJatXHZ2TyWLSce8ngWUD
btKhv5A04cvFHisMHiddHmVDS4EQcwJ9Xret3rayPcc74Ce9uxUTY+4fXcL5fVBWIt6T4EC6DuQP
vd+9iAya19IN0/MIZDs8 1uqHOw/gogsgQa3RKPX+3nRE YnE5jRPpE6arWFTLmuQmYzEQ2T8Hke9Gx
eCBV9oSSUXZ49nseeK187IKYlRmIK7PrER8zNXditZuY10OfMP78v+nwT8finuO14IzmRXU5eWY7j
Wh0JKdi0F04VIDXjawRbJ/ySeR71ote3MMvIOyEhv+t4vN6Y+3jo2ndXAhFLQ0R7rAkr+ksnS9dI
qdI3xZfgXT9atgFQkzIT73KHZtnIY9qV6qt0UjiTuM1zcnMtE5CzS3D+scmcg6nRzyvZc0St7yzT
1oBYUjNBB8KqDNz3/Z2t7+GGn9heXD4XZ3P+JrIfs+Ls25Vq2ce/CSd8bxfcz2AXsRSGrGrOIanr
vtY/Q9OUNhDmgR8OzP7jdi8wrOjGorEykYCkuDrtsAtmQPl2N6iJ4ZU38hnC76pN0zaQgqu/yTi5
wdrF7f1V+8SUYCWNqD5oc+8CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFM+NapRPq0rkPUA3TdAGx6k7WWDSMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3
DQEBBQUAA4ICAQAEVoleViGQQPt7MVdQW5W2vPOBInbIGzUma2BZz1qsyhg0UisqCOYexhRXalhX
ejAxWIEjIjo2+I4Ig6QUQ3s2s3E/UZyNnxQ4aspE9N45F0tRwnbokwNHmKbPdKKwvCvN/F848Fm3
q+K+GORroJPm1bIIyz4U4K+7UyhOwRJ/CIlL1JPEwlt/Pwphg/aKS6RE2plsjwjaINjukRz5W557
qD14RdgVrIQHt2Nc8vq1p3i4LhGJwUlkCSebLZ447m/lcn/Gn+sm7OmN+ackCE3Ol7Xj1iG19EMM
5zFoIRsHIu4C4HQQtfCDQSap0Gy7ExEbrKvSpOCw2bSfpFuy69BIUmTM1CTvzrKS1GsgkNIJEQZ
K2EqAr+LbSC3swD7gDev+SCyrULquYiySjkUH7RDTPTL6BCxrYE8Ip+1dAXV0PYqbg/XJ/st0ZJmG
KZrTH3ClBQQ25dj2ysEg+9YGcjGk6oJKhUOeJbCH+bM7sg31g9nRGmjhJUX2jPVmzaPuWcX2+2Vl
sNnzy4ur/MvC8FLPCU6l5ysLk5nQ5qcYgw10SgAXDoNNyxmSdPlSQ5CjvJr5HzCUMy/1ZAhuqBzT
wwVxEhJisNx0XaVH5MabnSVfv37m12D2WsKHEBcUdTvjG4vOeiR0LgqfRnSwtfQBeD19wvrY6h24
dzh1miMPJtDIKw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *CA CICCP Clase 3*

Issuer OU: *CICCP C.I.F. Q-2867009-I*

Issuer O: *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Issuer L: *Madrid*

Issuer ST: *Madrid*

Issuer C: *ES*

Issuer E: *pki@ciccp.es*

Subject CN: *CA CICCP Clase 3*

Subject OU: *CICCP C.I.F. Q-2867009-I*

Subject O: *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

Valid from: *Mon Aug 17 12:25:28 CEST 2009*

Valid to: *Sat Aug 17 12:35:26 CEST 2019*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D0:72:CE:FB:30:21:4A:27:14:4E:1C:78:D1:EC:9C:75:68:07:F7:40:82:DB:85:E1:81:B2:91:DF:9E:1D:46:84:3E:AA:B8:3E:36:02:6D:81:6D:A8:1C:9D:B1:BE:41:10:58:71:6C:78:B7:BB:60:91:A5:91:65:09:A7:A5:DE:FB:D6:1F:68:6A:F5:48:B9:24:30:57:F9:9E:1D:06:02:F0:EE:25:AB:57:1D:9D:93:C9:62:D2:71:EF:27:81:65:03:6E:D2:A1:BF:90:34:E1:CB:C5:1E:2B:0C:1E:27:5D:1E:65:43:4B:81:10:73:02:7D:5E:B7:AD:DE:B6:B2:3D:C7:3B:E0:2C:FD:BB:15:13:63:EE:1F:5D:C2:F9:7D:50:56:22:DE:93:E0:40:BA:0E:E4:0F:BD:DF:BD:88:0C:AE:D7:D2:0D:D3:F3:08:66:1F:35:BA:A1:CE:C3:F8:28:82:CA:90:6B:74:4A:3D:7F:B7:9D:11:18:9C:4E:63:44:FB:04:E9:AB:56:15:32:E6:B9:09:95:CC:44:36:4F:C1:E4:7B:D1:B1:78:20:55:F6:84:92:51:76:78:F6:7B:1E:78:AD:7C:EC:82:98:21:19:A5:2B:B3:EB:11:1F:33:35:77:62:B5:9B:98:D7:43:9F:30:FE:FC:BF:E9:F0:4F:C7:E7:B8:ED:78:23:39:91:5D:4E:5E:59:8E:E3:5A:1D:09:29:D8:B4:17:4E:15:20:35:E3:6B:04:5B:27:FC:92:71:1E:E5:A2:D7:B7:30:CB:C8:3B:21:21:BF:EB:78:BC:DE:98:FB:78:E8:DA:77:57:02:11:4B:43:44:7B:AC:09:2B:FA:4B:27:4B:D7:48:AB:82:37:C5:92:20:5D:3F:5A:B6:01:50:93:32:08:EF:72:87:66:D9:C8:63:DA:95:EA:AB:74:52:38:93:B8:CD:73:72:73:2D:13:90:B3:4B:70:FE:B1:C9:9C:83:A9:FC:CE:3B:D9:73:44:AD:EF:2C:D3:D6:80:58:52:33:41:07:C2:AA:0C:DC:F7:FD:9D:A2:EF:E1:86:9F:D8:5E:5C:3E:17:67:73:FE:26:B7:C9:B3:E2:EC:DB:95:6E:DA:8A:FF:09:27:7C:6F:17:F1:CF:60:17:B1:14:86:AC:6F:CE:7D:A9:EB:BE:D6:3F:43:D3:94:36:10:E6:81:1F:0E:CC:FE:E3:76:2F:30:AC:E8:C6:A2:B1:32:91:80:A4:B8:3A:ED:B0:0B:66:40:F9:76:37:A8:89:E1:95:37:F2:19:C2:EF:AA:4D:D3:36:90:82:AB:BF:C9:38:B9:C1:DA:C5:ED:FD:55:FB:C4:94:60:25:8D:A8:3E:68:7B:EF:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *CF:8D:6A:94:4F:AB:4A:E4:3D:40:37:4D:D0:06:C7:A9:3B:59:60:D2*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AE:6B:A1:14:86:B5:17:CD:68:88:7F:55:86:68:49:67:DD:C9:EB:46:F6:7A:9D:BF:59:3E:31:D2:D2:4E:95:37*

X509SubjectName

Subject CN: *CA CICCP Clase 3*

Subject OU: *CICCP C.I.F. Q-2867009-I*

Subject O: *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

8.2.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Key Usage	*[keyEncipherment]*	*true*
Key Usage	*[dataEncipherment]*	*true*
Key Usage	*[keyAgreement]*	*false*
Key Usage	*[keyCertSign]*	*false*
Key Usage	*[crlSign]*	*false*
Key Usage	*[encipherOnly]*	*false*
Key Usage	*[decipherOnly]*	*false*

8.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.2.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificate*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA CA CICCP Clase 3*

Service digital identities

X509SubjectName

Subject CN:	*CA CICCP Clase 3*
Subject OU:	*CICCP C.I.F. Q-2867009-I*
Subject O:	*CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*
Subject L:	*Madrid*
Subject ST:	*Madrid*
Subject C:	*ES*
Subject E:	*pki@ciccp.es*

X509SKI

X509 SK I	*z41qlE+rSuQ9QDdN0AbHqTtZYNI=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*
Status Starting Time	*2015-03-19T23:00:00Z*

8.2.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Key Usage	*[keyEncipherment]*	*true*
Key Usage	*[dataEncipherment]*	*true*
Key Usage	*[keyAgreement]*	*false*
Key Usage	*[keyCertSign]*	*false*
Key Usage	*[crlSign]*	*false*

Key Usage	[encipherOnly]	false
Key Usage	[decipherOnly]	false

8.2.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	Qualified Certificate
Name	[es]	Certificados Reconocidos emitidos por la CA CA CICCP Clase 3

Service digital identities

X509SubjectName

Subject CN:	CA CICCP Clase 3
Subject OU:	CICCP C.I.F. Q-2867009-I
Subject O:	CICCP - Colegio de Ingenieros de Caminos Canales y Puertos
Subject L:	Madrid
Subject ST:	Madrid
Subject C:	ES
Subject E:	pki@ciccp.es

X509SKI

X509 SK I	z41qlE+rSuQ9QDdN0AbHqTtZYNI=

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2013-07-07T00:00:00Z*

8.2.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Key Usage	*[keyEncipherment]*	*true*
Key Usage	*[dataEncipherment]*	*true*
Key Usage	*[keyAgreement]*	*false*
Key Usage	*[keyCertSign]*	*false*
Key Usage	*[crlSign]*	*false*
Key Usage	*[encipherOnly]*	*false*
Key Usage	*[decipherOnly]*	*false*

8.2.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificate*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA CA CICCP Clase 3*

Service digital identities

X509SubjectName

Subject CN:	*CA CICCP Clase 3*
Subject OU:	*CICCP C.I.F. Q-2867009-I*
Subject O:	*CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*
Subject L:	*Madrid*
Subject ST:	*Madrid*
Subject C:	*ES*
Subject E:	*pki@ciccp.es*

X509SKI

X509 SK I	*z41qlE+rSuQ9QDdN0AbHqTtZYNI=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2010-01-25T00:00:00Z*

9 - TSP: HEALTHSIGN, S.L.

.

TSP Name

Name	*[en]*	*HEALTHSIGN, S.L.*
Name	*[es]*	*HEALTHSIGN, S.L.*

TSP Trade Name

Name	*[en]*	*VATES-B17944554*
Name	*[en]*	*HEALTHSIGN, S.L.*
Name	*[es]*	*HEALTHSIGN, S.L.*
Name	*[en]*	*Col-legi Oficial de Infermeria de Lleida*
Name	*[es]*	*Col-legi Oficial de Infermeria de Lleida*
Name	*[en]*	*Col-legi Oficial de Infermeria de Girona*
Name	*[es]*	*Col-legi Oficial de Infermeria de Girona*
Name	*[en]*	*Col-legi Oficial de Infermeria de Tarragona*
Name	*[es]*	*Col-legi Oficial de Infermeria de Tarragona*
Name	*[en]*	*Col-legi Oficial de Metges de Lleida*
Name	*[es]*	*Col-legi Oficial de Metges de Lleida*
Name	*[en]*	*Col-legi Oficial de Metges de Girona*
Name	*[es]*	*Col-legi Oficial de Metges de Girona*
Name	*[en]*	*Col-legi Oficial de Metges de Tarragona*
Name	*[es]*	*Col-legi Oficial de Metges de Tarragona*
Name	*[en]*	*Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*
Name	*[en]*	*Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I*
Name	*[en]*	*Col-legi Oficial de Metges de Lleida – CIF Q2566001J*
Name	*[en]*	*Col-legi Oficial de Infermeria de Girona – CIF Q1766003F*

Name	[en]	Col-legi Oficial de Metges de Girona – CIF Q1766001J
Name	[en]	Col-legi Oficial de Metges de Tarragona – CIF Q4366001H

PostalAddress

Street Address	[en]	C/Albereda, 3-5, ático
Locality	[en]	Girona
State Or Province	[en]	Gerona
Postal Code	[en]	17004
Country Name	[en]	ES

PostalAddress

Street Address	[es]	C/Albereda, 3-5, ático
Locality	[es]	Girona
State Or Province	[es]	Gerona
Postal Code	[es]	17004
Country Name	[es]	ES

ElectronicAddress

URI	[en]	mailto:healthsign@healthsign.org
URI	[en]	http://www.healthsign.org

TSP Information URI

URI	[en]	http://www.healthsign.org/pub/eng
URI	[es]	http://www.healthsign.org

9.1 - Service (withdrawn): Certificado de Colegiado Reconocido emitido por CA CODILL CA

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA CODILL CA*

Name *[en]* *Qualified Member Certificate issued by CA CODILL CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *458154954257264109682702*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFHDCCBASgAwIBAgIKYQShPQAAAAAADjANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMCRVMx
KDAmBgNVBAoMH0hFQUxUSFNJR04gU0wg4oCTIENJRtBCMTc5NDQ1NTQxMDAuBgNVBAsTJ0FsYmVy
ZWRhIG51bS4gMy01LiBBdGljLi4xNzAwNCAtIEdJUk9OQTEWMBQGA1UEAxMNQUMgSEVBTFRIU0lH
TjAeFw0wOTA3MjIwODA5MDJaFw0yNDA3MjIwODE5MDJaMIGcMQswCQYDVQQGEwJFUzFFMEMGA1UE
CjwWQ29sLWxlZXkgT2ZpY2lhbCBkZSBlbmZlcm1cmlhIGRlIEcsZWlkYSDigJMgQ0lGIFEtMjU2
NjAwMy1GMTIwMAYDVQQLEyIQYWVyIENhc2Fub3ZhcyAzNyAtIGFsdGVsbCAyNTAwOCAtIExMRUlE
QTESMBAGA1UEAxMJQ09ESUxMIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6jkw
2A32ezTJEBxHqnEq2Mw4hkYIYAyeV4qWO+zxDYYipKE0AvpXxa4mcxg6ozQ4yevsv9mW/igxoVF
V2UIqUxG9A+OFgzIz/6Dw32Y5f5MMc7zcA7+1u6Bp7hdIMsTFAABA7zO3HbZjVT0bhnoZzXkOx
GrtYMJGkHTHe407cOC4snVluRMwf/QoZZ71fc7JA7fZzFCebY6PP11S6zRGc0SJlIB/pESFA0ksu
DPYIpx/JgYlX9pKaktEwrs4pFtOjR8x5nQ7gIX6i0BpFVY1n1Gb4CkThFWYHRVZk15QFRcX6o7Ys
fuymeBT6zU97KTS3fxH/B5ADZ4OyBr5AQIDAQABo4IBdzCCAXMwEgYDVR0TAQH/BAgwBgEB/wIB
AIDAdBgNVHQ4EFgQUsFjmBNUjzXo1WSEsabdEZc71S72wwCwYDVR0PBAQDAgGGMBAGCSsGAQQBgjcV
AQQDAgEAMFQGA1UdIARNMEswQQYKKwYBBAGB3nkBATAzMDEGCCsGAQUFBwIBFiVodHRwOi8vd3d3
LmhlYWx0aHNpZ24ub3JnL3JlcG9zaXRvcnkvMAYGBFUdIAAwGQYJKwYBBAGCNxQCBAweCgBTAHUA
YgBDAEEwHwYDVR0jBBgwFoAUC26TYI3IamDAKB+6s6974dNysXkwQAYDVR0fBDkwNzA1oDOgMYYv
aHR0cDovL3d3dy5oZWFsdGhzaWdub.m9yZy9yZXBvc2l0b3J5L2hlc2lj YSSjcmwwSwYIKwYBBQUH
AQEEPzA9MDsGCCsGAQUFBzAChi9odHRwOi8vd3dL mhlYWx0aHNpZ24ub3JnL3JlcG9zaXRvcnkv
aGVzaWNhLmNydDANBgkqhkiG9w0BAQUFAAOCAQEAXj+PG6V9fpmkLW61B1QY1GXs81KlhRcZ/d1f
n2ubBaCdD7/KCmTIm1yr1iÃaKJfb5jwADc80pB4PBcw37HposS3vW49rILhb5hD5vnKok6m/ePWNo
NTrzXO/ueMDrJ2rwk0utacgsicD4k/whbWZHRf5khEOj6k+swbwD6AphIbEdoSnS8877Pg0qwR
LO2oKz11zas+afyfqib+N6TuE8bYUCYaZMU4wJmE9OAXwxdT+shrzjfW3+OGa47Ctz6jeVubO+MN
znks8RZo8oStHkZldKAZNgbdme/8daKHCF12UnRjSFOQShfxEEzg1PnGSNiccHPN1wcJeDVM8KFt
Kw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *AC HEALTHSIGN*

Issuer OU: *Albereda num. 3-5. Atic. 17004 - GIRONA*

Issuer O: *HEALTHSIGN SL – CIF B17944554*

Issuer C: *ES*

Subject CN: *CODILL CA*

Subject OU: *Paer Casanovas 37 - altell 25008 - LLEIDA*

Subject O: *Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*

Subject C: *ES*

Valid from: *Wed Jul 22 10:09:02 CEST 2009*

Valid to: *Mon Jul 22 10:19:02 CEST 2024*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EA:39:30:D8:0D:F6:89:EC:D3:24:40:71:1E:A9:C4:AB:63:30:E2:19:18:21:80:32:79:5E:2A:58:EF:B3:C4:36:18:8A:92
:84:D0:0B:E9:5F:16:B8:99:CC:60:EA:8C:D0:E3:27:AF:B2:FF:66:5B:F8:A0:C6:85:45:57:69:49:89:E8:D4:C4:6F:40:F8:E1:60:8C:BA:FF:E8:3C:37:D9:8E:49:E4:C3:1C:ED:C7:00:EF:E2:EE:E8:1A:7B:85:D2:0C:B1:31:40:00:
10:3B:CC:ED:F8:85:98:D5:4F:48:61:9E:86:73:5C:A3:B1:1A:B7:D8:30:91:A4:1D:31:DE:E3:4E:DC:38:2E:2C:9D:59:6E:44:CC:1F:FD:0A:19:67:BD:5F:71:32:40:ED:F6:73:14:27:9B:63:A3:CF:D7:54:BA:CD:11:9C:D1:22:48
:94:1F:E9:11:21:40:D2:C9:2E:0C:F6:08:A7:1F:C9:81:89:57:F6:92:9A:92:D1:30:AE:CE:29:16:D4:23:47:CC:79:9D:0E:E0:21:7E:A2:D0:1A:45:55:8D:67:D4:66:F8:0A:44:E1:15:66:07:45:56:64:D7:94:05:45:E5:FA:A3:B6:2C:
7E:EC:A7:78:14:FA:CD:4F:7B:29:34:B7:7D:FC:47:FC:1E:40:0D:9E:0E:C8:1A:F9:01:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *B0:58:E7:04:D5:20:5E:84:D6:48:4B:1A:6D:D1:19:73:BD:52:EF:6C*

Certificate Policies	*Policy OID: 1.3.6.1.4.1.28537.1.1* *CPS pointer: http://www.healthsign.org/repository/* *Policy OID: 2.5.29.32.0*
Authority Key Identifier	*0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79*
CRL Distribution Points	*http://www.healthsign.org/repository/hesica.crl*
Authority Info Access	*http://www.healthsign.org/repository/hesica.crt*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C7:F6:82:27:03:47:4B:47:1C:14:4F:B8:B8:13:B3:9C:D9:69:53:7F:AD:59:5B:56:C8:06:B4:C5:3C:D1:A0:43*

X509SubjectName

Subject CN:	*CODILL CA*
Subject OU:	*Paer Casanovas 37 - altell 25008 - LLEIDA*
Subject O:	*Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

9.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.1.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA CODILL CA*

Name *[en]* *Qualified Member Certificate issued by CA CODILL CA*

Service digital identities

X509SubjectName

Subject CN: *CODILL CA*

Subject OU: *Paer Casanovas 37 - altell 25008 - LLEIDA*

Subject O: *Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*

Subject C: *ES*

X509SKI

X509 SK I *sFjnBNUgXoTWSEsabdEZc71S72w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-11-30T23:00:00Z*

9.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA CODILL CA*

Name *[en]* *Qualified Member Certificate issued by CA CODILL CA*

Service digital identities

X509SubjectName

Subject CN: *CODILL CA*

Subject OU: *Paer Casanovas 37 - altell 25008 - LLEIDA*

Subject O: *Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*

Subject C: *ES*

X509SKI

X509 SK I	*sFjnBNUgXoTWSEsabdEZc71S72w=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2010-10-01T00:00:00Z*

9.2 - Service (withdrawn): Qualified Member Certificate issued by CA CODITA CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Member Certificate issued by CA CODITA CA*
Name	*[es]*	*Certificado de Colegiado Reconocido emitido por CA CODITA CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *462319913310478852423687*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFHjCCBAagAwIBAgIKYeZpqAAAAAAABzANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMCRVMx
KDAmBgNVBAoMH0hFQUxUSFNJR04gU0wg4oCTIENJRiBCMTc5NDQ1NTQxMDAuBgNVBAs TJ0FsYmVy
ZWRhIG51bS4gMy01LiBBdGljLiAxNzAwNCAtIEdUk9OQTEWMBQGA1UEAxMNQUMgSEVBTFRIU0lH
TjAeFw0wNzA0MjYxMTA3MDhaFw0yMjA0MjYxMTE3MDhaMIGeMQswCQYDVQQGEwJFUzFGMEQGA1UE
CgwWQ29nZ.WxlZ2kgT2ZpY2lhbCBkZSBJbmZlcm1cmlhIGRlIFRhcnJhZ29uYSDgzJMgQ0IGIFE0
MzY2MDA1STEzMDEGA1UECxMqQXZkYS4gUGF1IENhc2Fscy4gMTMtNWUtIDQzMDAzIC0gVEFSUkFH
T05BMRIwEAYDVQQDEwlDT0RJVEEgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8
by5Y+/dia3Pye7ncuyKtludvRERajV0dyQHzRMlaf2bxEbbocLH3jmpEGqeka6D74fX/yUOcAgo
nIxvTZ1eASceeMo8mPgp4AQVzvIENypWutkVDp4wbZcXKL1Aw0huiov1IPDbzLHFtszvBSxkYAcC
fwNeEBDx55iTfvIFlSxU7JGhmdZLwJJUMY8gvY+H6JEmCEkHgZvZLzP1OsjpLYYEzo7CxbY7y7lE
QLbtFGhAG4J0T6OfOnrIr+zMZK8MtBTKaWav6XZEXRTvZXDC27U2pK9LxFmqG86yZ3IAtrOv7bHe
VS4J27D/8oZM10isjO/3rkPFhfYssBequu01AgMBAAGjggF3MIIBczASBgNVHRMBAf8ECDAGAQH/
AgEAMB0GA1UdDgQWBBRLf8wvHh1gKuozSS7CdHBEjKsRDALBgNVHQ8EBAMCAYYwEAYJKwYBBAGC
NxUBBAMCAQAwVAYDVR0gBE0wSzBBBgorBgEEAYHeeQEBMDMwMQYIKwYBBQUHAgEWJWh0dHA6Ly93
d3cuaGVhbHRoc2lnbi5vcmcvcmVwb3NpdG9yeS8wBgYEVR0gADAZBgkrBgEEAYI3FAIEDB4KAFMA
dQBiAEMAQTAfBgNVHSMEGDAWgBQLbpNiXchqYMAoH7qzr3vh03Kxe1TBABgNVHR8EOTA3MDWgM6Ax
hh9odHRwOi8vd3d3L mhlYWxlaHNpZ2Ub3JnL3JlcG9zaXRvcnkvaGVzaWNhLmNybDBLBggrBgEF
BQcBAQQ/MD0wOwYIKwYBBQUHMAKGL2h0dHA6Ly93d3cuaGVhbHRoc2lnbi5vcmcvcmVwb3NpdG9y
eS9oZXNpY2EuY3J0MA0GCSqGSIb3DQEBBQUAA4IBAQBYmYpxnLs7664LNG5Ixpguhd+gDKiPUsKK
bCsbqWGOKCbHmZKzmG5AXxcL p6ka3obLx8tnrbW3kqGmaSS8Y88TUAapbFp9BaPJ8WTawJZAkH2g
9KFL11UPnn/4cIRIqRw2n0chUDbF+HCiSgOWj6Pq+bgcgg6KHucIPwXN33T7wTkrZQzNpKnD/
/X5PsAFB49uHZiFwYqr3CMCLDXXb7yYrdKJrhdezNSQRSomd5QCTh2VsvRFKr4PTArlOG7jl8PBp
hjV3aelLOlgyLo3ZylvcNStckGOyGUFYE/RKeqGE5OgAHmAm+diZpPTB+LDLsBQaQ10KEEFAIXt
CaJx

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *AC HEALTHSIGN*

Issuer OU: *Albereda num. 3-5. Atic. 17004 - GIRONA*

Issuer O: *HEALTHSIGN SL – CIF B17944554*

Issuer C: *ES*

Subject CN: *CODITA CA*

Subject OU:	*Avda. Pau Casals. 13-5e. 43003 - TARRAGONA*
Subject O:	*Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I*
Subject C:	*ES*
Valid from:	*Thu Apr 26 13:07:08 CEST 2007*
Valid to:	*Tue Apr 26 13:17:08 CEST 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:6F:2E:58:FB:F7:62:6B:73:F2:7B:B9:DC:BB:22:AD:22:E7:6F:44:44:5A:8D:57:F4:77:24:07:CD:13:25:69:FD:9B:C4:46:DB:A1:C2:C7:DE:39:A9:10:6A:9E:91:AE:83:EF:87:D7:FF:25:0E:C4:08:28:9C:8C:6F:4D:9D:5E:01:27:1E:AC:CA:3C:98:F8:23:E0:04:15:CE:F9:44:37:FA:56:BB:A5:43:A7:8C:1B:67:15:CA:2E:20:30:3A:1B:A2:A2:FD:48:3C:38:73:94:B1:C5:B6:CC:EF:05:2C:64:54:07:02:7F:03:5E:10:10:F1:E7:98:93:7E:F2:05:7D:2C:54:EC:91:A1:99:D6:4B:C0:92:54:31:8F:20:BD:8F:87:E8:91:26:08:49:07:81:9B:D9:2F:33:F5:3A:C8:E9:2D:86:04:CE:8E:C2:C5:B6:3B:CB:B9:44:40:B6:ED:14:66:C0:1B:82:74:4F:A3:9F:3A:7A:C8:AF:EC:CC:64:AF:0C:B4:14:CA:69:66:AF:E9:76:44:5D:14:EF:65:70:C2:DB:B5:36:A4:AF:4B:C4:59:AA:1B:CE:B2:67:72:00:B6:B3:AF:EE:11:DE:55:2E:09:DB:B0:FF:F2:86:4C:D7:48:AC:8C:EF:F7:AE:43:C5:85:F6:2C:B0:17:AA:8A:E3:B5:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*4B:7F:CC:2F:1E:1D:60:2A:E7:1D:49:2E:C2:74:7B:41:12:32:B1:44*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.28537.1.1* *CPS pointer: http://www.healthsign.org/repository/* *Policy OID: 2.5.29.32.0*
Authority Key Identifier	*0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79*
CRL Distribution Points	*http://www.healthsign.org/repository/hesica.crl*
Authority Info Access	*http://www.healthsign.org/repository/hesica.crt*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F8:07:01:AE:DC:23:5D:23:71:03:C1:08:61:7D:94:46:5D:41:3C:40:37:17:0B:59:9E:AB:DD:64:8D:33:56:5E*

X509SubjectName

Subject CN:	*CODITA CA*
Subject OU:	*Avda. Pau Casals. 13-5e. 43003 - TARRAGONA*
Subject O:	*Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

9.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.2.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Member Certificate issued by CA CODITA CA*
Name	*[es]*	*Certificado de Colegiado Reconocido emitido por CA CODITA CA*

Service digital identities

X509SubjectName

Subject CN:	*CODITA CA*
Subject OU:	*Avda. Pau Casals. 13-5e. 43003 - TARRAGONA*
Subject O:	*Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I*
Subject C:	*ES*

X509SKI

X509 SK I	*S3/MLx4dYCrnHUkuwnR7QRIysUQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-11-30T23:00:00Z*

9.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	Qualified Member Certificate issued by CA CODITA CA
Name	[es]	Certificado de Colegiado Reconocido emitido por CA CODITA CA

Service digital identities

X509SubjectName

Subject CN:	CODITA CA
Subject OU:	Avda. Pau Casals. 13-5e. 43003 - TARRAGONA
Subject O:	Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I
Subject C:	ES

X509SKI

X509 SK I	S3/MLx4dYCrnHUkuwnR7QRIysUQ=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision
Status Starting Time	2009-09-09T00:00:00Z

9.3 - Service (withdrawn): Qualified Member Certificate issued by CA COMLL CA

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Member Certificate issued by CA COMLL CA
Name	[es]	Certificado de Colegiado Reconocido emitido por CA COMLL CA

Service digital identities

Certificate fields details

Version:	3
Serial Number:	863557758202410707189 86

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFETCCA/mgAwIBAgIKEklblgAAAAAACjANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMCRVMx
KDAmBgNVBAoMH0hFQUxzUSFNJR0Ag U0wgdoCTIENJRzBCMTc5NDQ1NTQxMDAuBgNVBAs TI0FsYmVy
ZWRhIG5tbS4gMy01LiBBdGlJLzAxNzAwNCAtIEdUk9OQTEWMBQGA1UEAxMNQUMgSEVBTFRIU0lH
TjAeFw0wNzA0MjYxNzM0NDlaFw0yMjA0MjYxNzQ0NDlaMIGRMQswCQYDVQQGEwJFUzE/MD0GA1UE
Cgw2Q29sL WxJZ2kgT2ZpY2lhbCBkZSBNZXRnZXMgZGUg TGxlaWRhIOKAkyBDSUYgUT11NjYwMDFK
MS4wLAYDVQQLEyVSYW1ibGEgQXlhZ28gMTQuIHByY WwuID1MDAyIC0gTExFSURMREwDwYDVQQD
EwhDT01MTCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPk97uXbsInXj7X3+atj
obz6+/wuqX/P2bzxO7mb0Or1LOKwIu43jk308gN5xzzWh/WyhYsn7vwPqnm+IWMX160uIhh5Qt9J
2MaPLpbCQUwhYeaFybXHvOqfirawygLGRMb4kZqPwWZIwOe8MNI9uqfCRoaXcIQaeBgUP4/awY0I
S76vS3k+JhsXfzvzt9qLyyLt0N1HahDHmIxqI5laOyoZBZY8HL0kFXaRJQsPCTW36fwAe4Cefz9
UAxa0umtj6U+hFfvxx+A9D9EWuerabFSrBtpGmFtfXLUjfZopGsasMv9d9m7U5QB4D4VAb&GUynu
zL24y2IzTdvSS0M7tH0CAwEAAaOCAXcwggFzMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYE
FFTWNyoCQokdh9tVwdx16Fv/AJrhMAsGA1UdDwQEAwIBhjAQBgkrBgEEAYI3FQEEAwIBADBUBgNV
HSAETTBLMEEGCisGAQQBgd55AQEwMzAxBggrBgEFBQcCARYlaHR0cDovL3d3dy5oZWFsdGhzaWdu
Lm9yZy9yZXBvc2l0b3I5LzAGBgRVHSAAMBkGCSsGAQQBgzUAgQMHgoAUwB1AGIAQwBBMBBGA1Ud
IwQYMBaAFAtuk2JdyGpgwCgfurOve+HTcrF5MEAGA1UdHwQSMDcwNaAzoDGGL2h0dHA6Ly93d3cu
aGVhbHRoc2lnbi5vcmcvcmVwb3NpdG9yeS9oZXNpY2EuY3JsMEsGCCsGAQUFBwEBBD8wPTA7Bggr
BgEFBQcwAoYvaHR0cDovL3d3dy5oZWFsdGhzaWduLm9yZy9yZXBvc2l0b3I5L2hlc2lyYS5jcnQw
DQYJKoZIhvcNAQEFBQADggEBAKKF1JigWr14FqwTcAU3XojyCuGmxnYcOyKuFMHsEQdTACRZYdhn
rXJaRLoDoB3Z3+XvtMWA2aqTIOOJ1lq2rO0ddf9iTYF2jgr+VA/+3dhGTLHqhG66U/hAh1RImqH
2pmSRpRYlN2XMrAKmGAcI+JLaz0801HoevDV6u6kg4GzZ0yzRKU60RKVxesEegl8CrzQR571eNq1
EL4xYECISSzzFujrfiUdNayAxN0bDZShHvYuylfjo7K6TAMVJkWQbUCmBGpMFlNnWsAa6CIC2QYU
yycmZxAzfvdFOmu7QQTWHPSSN/wsJTbBWSs/OTJW2XK5qKF0kPnrYSXxkPqwZyU=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *AC HEALTHSIGN*

Issuer OU: *Albereda num. 3-5. Atic. 17004 - GIRONA*

Issuer O: *HEALTHSIGN SL – CIF B17944554*

Issuer C: *ES*

Subject CN: *COMLL CA*

Subject OU: *Rambla Arago 14. pral. 25002 - LLEIDA*

Subject O: *Col-legi Oficial de Metges de Lleida – CIF Q2566001J*

Subject C: *ES*

Valid from: *Thu Apr 26 19:34:49 CEST 2007*

Valid to: *Tue Apr 26 19:44:49 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F9:3D:EE:E5:DB:B0:89:D7:8F:B5:F7:F9:AB:63:A1:BC:FA:FB:FC:2E:A9:7F:CF:D9:BC:F1:3B:B9:9B:D0:EA:F5:2C
:E2:B0:22:EE:37:8E:4D:F4:F2:03:79:C7:3C:D6:87:F5:B2:85:8B:27:EE:FC:0F:AA:79:BE:D5:63:17:D7:AD:2E:22:18:79:42:DF:49:D8:C6:8F:2E:96:C2:41:4C:21:61:E6:85:C9:B5:C7:BC:EA:9F:AD:AC:32:80:B1:91:31:BE:24
:66:A3:F0:59:F6:65:C0:E7:BC:30:D2:3D:BA:A7:C2:46:86:97:78:84:1A:78:18:14:3F:8F:DA:C1:8D:08:4B:BE:AF:4B:79:3E:26:1B:17:7F:3B:F3:B7:DA:8B:CB:22:ED:D0:DD:47:6A:10:C7:98:8C:6A:97:99:5A:3B:2A:19:05:9
6:3C:1C:BD:24:15:76:91:25:0B:22:3C:24:D6:DF:A7:F0:01:EE:02:79:FC:FD:50:0C:5A:3A:E9:AD:8F:A5:3E:84:57:EF:BF:1F:80:F4:39:7D:11:6B:9E:AD:A6:C4:4A:B0:5B:A4:69:85:75:72:D4:8C:56:68:A4:6B:1A:B0:CB:FD:
77:D9:BB:53:94:01:E0:3E:15:01:B9:06:53:29:EE:CC:BD:B8:CB:62:33:4D:DB:D2:4B:43:3B:7C:7D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *54:D6:37:2A:02:42:89:1D:87:DB:55:C1:DC:75:E8:5B:FF:00:9A:E1*

Certificate Policies

Policy OID: 1.3.6.1.4.1.28537.1.1

CPS pointer: http://www.healthsign.org/repository/

Policy OID: 2.5.29.32.0

Authority Key Identifier *0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79*

CRL Distribution Points *http://www.healthsign.org/repository/hesica.crl*

Authority Info Access *http://www.healthsign.org/repository/hesica.crt*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *80:D0:B3:C8:B8:C3:1C:D3:3E:36:0E:1A:DA:20:8A:37:12:EF:FE:09:1B:B2:84:40:52:A7:35:F7:B4:5C:CC:42*

X509SubjectName

Subject CN: *COMLL CA*

Subject OU: *Rambla Arago 14. pral. 25002 - LLEIDA*

Subject O: *Col-legi Oficial de Metges de Lleida – CIF Q2566001J*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

9.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.3.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name *[en]* *Qualified Member Certificate issued by CA COMLL CA*

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA COMLL CA*

Service digital identities

X509SubjectName

Subject CN:	*COMLL CA*
Subject OU:	*Rambla Arago 14. pral. 25002 - LLEIDA*
Subject O:	*Col-legi Oficial de Metges de Lleida – CIF Q2566001J*
Subject C:	*ES*

X509SKI

X509 SK I	*VNY3KgJCiR2H21XB3HXoW/8AmuE=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*
Status Starting Time	*2015-11-30T23:00:00Z*

9.3.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Member Certificate issued by CA COMLL CA*
Name	*[es]*	*Certificado de Colegiado Reconocido emitido por CA COMLL CA*

Service digital identities

X509SubjectName

Subject CN:	*COMLL CA*
Subject OU:	*Rambla Arago 14. pral. 25002 - LLEIDA*
Subject O:	*Col-legi Oficial de Metges de Lleida – CIF Q2566001J*
Subject C:	*ES*

X509SKI

X509 SK I	*VNY3KgJCiR2H21XB3HXoW/8AmuE=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2009-09-09T00:00:00Z*

9.4 - Service (withdrawn): Qualified Member Certificate issued by CA CODIGI CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Member Certificate issued by CA CODIGI CA*

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA CODIGI CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *80595025348812701958152*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFEjCCA/qgAwIBAgIKEREQqQAAAAAACDANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMCRVMx
KDAmBgNVBAoMH0hFQUxUSFNJR04gU0wg4oCTIENJRiBCMTc5NDQ1NTQxMDAuBgNVBAsTJ0FsYmVy
ZWRhIG51bS4gMy01LiBBdGljLiAxNzAwNCAtIEdlUk9OQTEWMBQGA1UEAxMNQUMgSEVBTFRIU0lH
TjAzFw0wNzA0MjYxMTU2NDNaFw0yMjA0MjYxMjAzNDNaMIG5MQswCQYDVQQGEwJFUzFDMEEGA1UE
Cgw6Q29sLWxlZ2kgT2ZpY2lhbCBkZSBJbmZlcm1lcmlhIGRlIEdpcm9uYSDigJMgQ0lGIFExNzY2
MDAzRjEqMCgGA1UECxMhQWxiZXJlZGEulDMtNS4gM2EulDE3MDA0IC0gR0lST05BMRIwEAYDVQQD
EwlDT0RJR0kgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDLVdzFW9kZ+rVcfgZ6
v2T87yS3T2riExdUaxpA3W4OahuSwopJzrarU/99fsW/5w7PnzkfvAOcH28WF/M0d5mxw3Am9OnJn
4pmJRSkUvSe4IsuU2WvqoQUTiOZclEICKz0WxUhOi59IBlHzXgIG2gZdcH6jQy8C0A4qzl7VWVRe
y14vcL4Oc6dca8XwedRxUJ83FT+uiWMRmkQWiARWIFsZmFk9p8rk4gp5DGPQLtX2VrhPyDlZgqNM
zQzLak8R7jwgdPQvVVFn5ynOCqxtuDX7P41i8wSEznPH7zQgj0Clm0cFlL7kuA25RVL2HnRwte1
N+sxSZebuKXyt1x43pAdHAgMBAAGjggF3MIIBczASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1UdDgQW
BBTmgrVm9IXXndu/lGuZbkk3ICLxVDALBgNVHQ8EBAMCAYYwEAYJKwYBBAGCNxUBBAMCAQAwVAYD
VR0gBE0wSzBBBgorBgEEAYHecQEBMDMwMQYIKwYBBQUHAgEWJWh0dHA6Ly93d3cuaGVhbHRoc2ln
bi5vcmcvcmVwb3NpdG9yeS8wBgYEVR0gADAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMAQTAfBgNV
HSMEGDAWgBQLbpNiXchqYMAoH7qzr3vbt03KxeTBABgNVHR8EOTA3MDWgM6Axhr9odHRwOi8vd3d3
LmhlYWxtaHNpZ24tb3InL3IcG9zaXRvcnkvaGVzaWNhLmNybDBLBggrBgEFBQcBAQQ/MDBwOwYI
KwYBBQUHMAKGL2h0dHA6Ly93d3cuaGVhbHRoc2lnbi5vcmcvcmVwb3NpdG9yeS9oZXNpY2EuY3J0
MA0GCSqGSIb3DQEBBQUAA4IBAQAQ2yCb+2qbN+gV1QMVAzhruNmHLy7H2dFJ/nomP6gmqcBI/Hz/
18+xpUTM9JDFeebrppUK+Wu1nphgFGhTm1q1AeyDdTi47A4eDRfQ3u0U/T1CYyS2Q6eW+u3Vjdmbr
NgG+W9NbH0wkY5Z841Xyz5QrAHRpAwarnW5L1YvKk7YSo11TfinAoseNZ/NXH0HFCgtQVytrDbst
+PHMwuxrd+X4irBpzUxT0oCWnDOA5FgNscdScFkN45cx4pLiWEqeM3pyx8F5Rzz4WtiWiNvhRIjG
qpwqV58kis4bfWOqkrQtdW03NA6Annr2h8SdEMwpflKQTD5zvqaazOEhxIA+uPPY

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *AC HEALTHSIGN*

Issuer OU: *Albereda num. 3-5. Atic. 17004 - GIRONA*

Issuer O: *HEALTHSIGN SL – CIF B17944554*

Issuer C: *ES*

Subject CN: *CODIGI CA*

Subject OU: *Albereda. 3-5. 3a. 17004 - GIRONA*

Subject O: *Col-legi Oficial de Infermeria de Girona – CIF Q1766003F*

Subject C: *ES*

Valid from: *Thu Apr 26 13:53:43 CEST 2007*

Valid to: *Tue Apr 26 14:03:43 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:55:DC:C5:5B:D9:19:FA:B5:5C:7E:06:7A:BF:64:FC:EF:24:B7:7D:3D:AB:88:4C:78:51:AC:69:03:75:B8:39:A8:6E:4B:0A:29:27:3A:DA:AD:47:FD:66:C5:B9:C3:B3:E7:CC:97:6F:00:E7:07:DB:C5:85:FC:CD:1D:E6:6C:70:DC:09:BD:3B:12:27:E2:99:89:45:29:14:BD:27:B8:22:CB:94:D9:6B:EA:A1:05:13:88:E6:5C:94:49:42:2B:3D:16:C5:48:4E:8B:9F:49:04:81:F3:5E:02:06:DA:06:5D:70:7E:A3:43:2F:02:D0:0E:2A:CE:5E:D5:59:54:5E:CB:5E:2F:70:BE:0E:73:A7:5C:6B:C5:F0:79:D4:71:50:9F:37:15:3F:AE:89:63:11:9A:44:16:88:04:56:94:5B:19:98:59:3D:A7:CA:E4:E2:0A:79:0C:63:D0:2E:B5:F6:56:B8:4F:C8:32:19:82:A3:4C:CD:0C:CB:6A:4F:11:EE:3C:20:74:F4:2F:55:51:67:E7:29:CE:0A:AC:6D:B8:35:FB:3F:8D:62:F3:04:84:CE:73:C7:EF:34:20:8F:40:A5:9B:47:05:94:BE:DF:92:E0:36:E5:15:4B:D8:79:D1:C2:D7:B5:37:EC:52:65:E6:EE:29:7C:AD:D7:1E:37:A4:07:47:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

E6:81:F5:66:F5:F5:D7:9D:DB:BF:94:6B:99:6E:49:37:20:22:F1:54

Certificate Policies

Policy OID: 1.3.6.1.4.1.28537.1.1

CPS pointer: http://www.healthsign.org/repository/

Policy OID: 2.5.29.32.0

Authority Key Identifier

0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79

CRL Distribution Points

http://www.healthsign.org/repository/hesica.crl

Authority Info Access

http://www.healthsign.org/repository/hesica.crt

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

E2:2F:28:CC:4C:F2:3F:D3:2B:9B:C1:93:04:A9:91:82:00:8A:BF:69:65:4D:CA:42:BA:65:CC:9B:FA:10:D9:D4

X509SubjectName

Subject CN:

CODIGI CA

Subject OU:

Albereda. 3-5. 3a. 17004 - GIRONA

Subject O:

Col-legi Oficial de Infermeria de Girona – CIF Q1766003F

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

9.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

9.4.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Member Certificate issued by CA CODIGI CA

Name [es] Certificado de Colegiado Reconocido emitido por CA CODIGI CA

Service digital identities

X509SubjectName

Subject CN: CODIGI CA

Subject OU: Albereda. 3-5. 3a. 17004 - GIRONA

Subject O: Col-legi Oficial de Infermeria de Girona – CIF Q1766003F

Subject C: ES

X509SKI

X509 SK I 5oH1ZvX1153bv5RrmW5JNyAi8VQ=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased

Status Starting Time 2015-11-30T23:00:00Z

9.4.3 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Member Certificate issued by CA CODIGI CA

Name [es] Certificado de Colegiado Reconocido emitido por CA CODIGI CA

Service digital identities

X509SubjectName

Subject CN: *CODIGI CA*

Subject OU: *Albereda. 3-5. 3a. 17004 - GIRONA*

Subject O: *Col-legi Oficial de Infermeria de Girona – CIF Q1766003F*

Subject C: *ES*

X509SKI

X509 SK I *5oH1ZvX1153bv5RrmW5JNyAi8VQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-09-09T00:00:00Z*

9.5 - Service (withdrawn): Qualified Member Certificate issued by CA COMG CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Member Certificate issued by CA COMG CA*

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA COMG CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *458579612176927755862027*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFDTCCA/WgAwIBAgIKYRumjQAAAAAACzANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMCRVMx
KDAmBgNVBAoMH0hFQUxUSFNJR04gU0wg4oCTIENJRiBCMTc5NDQ1NTQxMDAuBgNVBAsTJ0FsYmVy
ZWRhIG51bS4gMy01LzBBdGIjLzAxNzAwNCAtIEdJUk9OQTEWMBQGA1UEAxMNQUMgSEVBTFRlU0lH
TjAzFw0wNzA0MjcwNzM0MTdaFw0yMjA0MjcwNzQ0MTdaMIGNMQswCQYDVQQGEwJFUzEMD0GA1UE
Cgw2Q29sLWxlZ2kgT2ZpY2lhbCBkZSBNZXRnZXMgZGUgR2lyb25hIOKAkyBDSUYgUTE3NjYwMDFK
MSswKQYDVQQLEyJBbGJlcmVkYSAzLTUulEF0aWMuIDE3MDA0lC0gR0lST05BMRAwDgYDVQQDEwdD
T01HIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArDDAJf0ZJ8g71LxKhEi6/OkH
wiNuAIoyZzR8fQFJ02T/xZTguu5n6RjVS7kzBg3zZqcR4yUBPesyMmxB4CxZXqmG2c7m3zmmnG9
VRFyfTOY6kGLM62NngOPbHAN6Hf7wDcDc2vQXcgHw0MtVy5+alZwf3vZwtJPEzMBILfEuTGiPPmP
1IL5hDFTRVHVNUcOLH3VWFTCm0LgHHJLtPxFDW8wWsC/wPQ7SHtlk0mrKmXSoiqKPpVu2FcZXfWf
Lb6Ul6WWHysm+kG/fUScCUDV0/cIPgfxnU3T1yOZd8UXlaz8ywCjg1UGrsu18Kd5dzQGNXcXCRWLw
JrKIYZp8sTs45wIDAQABo4IBdzCCAXMwEgYDVR0TAQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUGVEO
b9DrltgdBHZ3WYnOOrfTL1+owCwYDVR0PBAQDAgGGMBAGCNsGAQQBgjcVAAQDAgEAMFQGA1UdIARN
MEswQQYKKwYBBAGB3nkBATAzMDEGCCsGAQUFBwIBFiVodHRwOi8vd3d3LmhlYWx0aHNpZ24ub3Jn
L3JlcG9zaXRvcnkvMAYGBFUdIAAwGQYJKwYBBAGCNxQCBAweCgBTAHUAYgBDAEEwHwYDVR0jBBgw
FoAUC26TYl3lamDAKB+6s6974dNysXkwQAYDVR0fBDkwNzA1oDOgMYYvaHR0cDovL3d3dy5oZWFs
dGhzaWduLm9vZy9yZXBvc20b3J5L2hlc2lYS5zmwwSwYIKwYBBQUHAQEPzA9MDsGCCsGAQUF
BzAChi9odHRwOi8vd3d3LmhlYWx0aHNpZ24ub3JnL3JlcG9zaXRvcnkvaGVzaWNhLmNydDANBgkq
hkiG9w0BAQUFAAOCAQEABo31GA43/wmzvd6zJ5HmOJoncAge4FSqJ1XKEvJIq2cVQ0BoL/609TcZ
NpN7VRMeyxRzvdHolSKXpt7RtsZ+H+tzLdmn0ucG2A+j0AvTC20hPWLkpX9ckAojMPhSzoIlgCX
mZcikk16YKRqnkqMt5jVosDEOtWR+iLplRsybgrOupwzDXR4XRFSHWY/QPRQo19Y95g7QSaQgf8Y
x+WIWSpIufqhP7JOMpIsq3fOZK+4N2H/7PO2Ps00JN0XV0SGl8thcezIYvC7iqBtElRGNZrR0jKy
qUEzSKdDVl87srqMHI3J4Gn3f8vgLG5OswVxBTU9zDTiY3BtwMbobiYhKA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *AC HEALTHSIGN*

Issuer OU:	*Albereda num. 3-5. Atic. 17004 - GIRONA*
Issuer O:	*HEALTHSIGN SL – CIF B17944554*
Issuer C:	*ES*
Subject CN:	*COMG CA*
Subject OU:	*Albereda 3-5. Atic. 17004 - GIRONA*
Subject O:	*Col-legi Oficial de Metges de Girona – CIF Q1766001J*
Subject C:	*ES*
Valid from:	*Fri Apr 27 09:34:17 CEST 2007*
Valid to:	*Wed Apr 27 09:44:17 CEST 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:30:C0:25:FD:19:27:CA:BB:D4:BC:4A:84:48:BA:FC:E9:07:C2:24:A1:B8:09:49:A3:26:73:47:C2:10:17:5D:36:4F:FC:59:4E:0B:A8:E6:7E:91:8D:54:BB:D1:C0:60:DE:26:6A:71:1E:32:50:13:DE:BE:33:27:C4:1E:02:C5:95:EA:98:6D:9C:EE:6D:F3:9A:61:BD:55:11:72:7D:33:98:EA:41:8B:33:AD:8D:9E:03:8F:6C:70:0D:E8:77:FB:C0:37:03:73:6B:D0:5D:C8:07:C3:43:2D:57:2E:7E:6A:56:70:7F:7B:D9:C2:D2:4F:13:33:01:20:B7:C4:B9:31:A2:3C:F9:8F:D4:82:F9:84:31:53:45:51:D5:35:47:8E:2C:7D:D5:58:54:C2:9B:42:E0:1C:72:4B:B4:FC:45:0D:6F:30:5A:C0:BF:C0:F4:3B:48:7B:65:93:49:AB:2A:65:D2:A2:2A:8A:3E:95:6E:D8:57:19:5D:F5:9F:2D:BE:94:E9:65:87:CA:C9:BE:90:6F:DF:53:97:02:50:35:74:FD:C2:0F:80:8C:67:53:74:F5:C8:E6:5D:F1:45:E5:6B:3F:32:C0:28:E0:D5:41:AB:B2:ED:7C:29:DE:5D:CD:01:8D:5D:C5:C2:45:62:F0:26:B2:A5:61:9A:7C:B1:37:B8:E7:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*19:51:0E:6F:D0:EB:96:D8:1D:04:76:76:59:89:CE:39:F4:CB:D7:EA*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.28537.1.1* *CPS pointer: http://www.healthsign.org/repository/* *Policy OID: 2.5.29.32.0*
Authority Key Identifier	*0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79*
CRL Distribution Points	*http://www.healthsign.org/repository/hesica.crl*
Authority Info Access	*http://www.healthsign.org/repository/hesica.crt*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*98:1F:E6:9D:F6:31:4B:83:0B:F9:94:91:FF:81:29:AC:D7:C0:AA:30:53:59:4E:1C:31:07:56:15:3B:C8:E0:60*

X509SubjectName

Subject CN:	*COMG CA*
Subject OU:	*Albereda 3-5. Atic. 17004 - GIRONA*
Subject O:	*Col-legi Oficial de Metges de Girona – CIF Q1766001J*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI [en] *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI [es] *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

9.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.5.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Member Certificate issued by CA COMG CA*

Name [es] *Certificado de Colegiado Reconocido emitido por CA COMG CA*

Service digital identities

X509SubjectName

Subject CN: *COMG CA*

Subject OU: *Albereda 3-5. Atic. 17004 - GIRONA*

Subject O: *Col-legi Oficial de Metges de Girona – CIF Q1766001J*

Subject C: *ES*

X509SKI

X509 SK I *GVEOb9DrltgdBHZ2WYnOOfTL1+o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-11-30T23:00:00Z*

9.5.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Member Certificate issued by CA COMG CA*
Name	*[es]*	*Certificado de Colegiado Reconocido emitido por CA COMG CA*

Service digital identities

X509SubjectName

Subject CN:	*COMG CA*
Subject OU:	*Albereda 3-5. Atic. 17004 - GIRONA*
Subject O:	*Col-legi Oficial de Metges de Girona – CIF Q1766001J*
Subject C:	*ES*

X509SKI

X509 SK I	*GVEOb9DrltgdBHZ2WYnOOfTL1+o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-09-09T00:00:00Z*

9.6 - Service (withdrawn): Qualified Member Certificate issued by CA COMT CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Member Certificate issued by CA COMT CA*
Name	*[es]*	*Certificado de Colegiado Reconocido emitido por CA COMT CA*

Service digital identities

Certificate fields details

Version:

3

Serial Number:

45943967641971572133070 0

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFGjCCBAKgAwIBAgIKYUpGVwAAAAAADDANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMCRVMx
KDAmBgNVBAoMH0hFQUxUSFNJR04gU0wg4oCTIENJRiBCMTc5NDQ1NTQxMDAuBgNVBAsTJ0FsYmVy
ZWRhIG51bS4gMy01LiBBdGljLiAxNzAwNCAtIEdJUk9OQTEWMBQGA1UEAxMNQUMgSEVBTFRlU0lH
TjAeFw0wNzA0MjcwODI1MTJaFw0yMjA0MjcwODM1MTJaMIGaMQswCQYDVQQGEwJFUzFCMEAGA1UE
Cgw5Q29sL WxlZ2kgT2ZpY2lhbCBkZSBNZXRnZXMgZGUgVGFvcmFnb25hIOKAkyBDSUYgITQzNjYw
MDFlMTUwMwYDVQQLEyxWaWEgSW1wZXJpIFJvbWEgbi4gMTEgYmluLiA0MzAwMyAtIFRBUlUlBR09O
QTEQMA4GA1UEAxMHQ09NVCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANroVyKZ
CD+PNFi3J6q6RyZLmSz4TCtcjryVyfgEvDt1B1XHyqtYzK6Q3CZr0QVaTf6qnwY+R8+yv7vMnnwN
hXC3gd3sc21AGe45KKdI1rTkV8oB4/+uUzZMA54rdZchnq/SVavtStpYFwpr/6MIwsxY9rr7T7d
qqNqC4NddgWVc8tyZND39BqOE2zhHsNmc8EQ3Db6QNGIHDBB7oquBvvRc2pJbKPKJpR83U/kiCKU
Z4+Mk4RPZOEecIyndw1T9jjXH7O0pFuB2vrOO4MMoBAe3wq+GrAMklB2xYCJt0Gx2397RPI2uHxu
Diavy/r+K6ZJyVI/+i7X7T1lj7iOtDcCAwEAAaOCAXcwggFzMBIGA1UdEwEB/wQIMAYBAf8CAQAw
HQYDVR0OBBYEFKdm9SksD8MDkKWYcmWBbBFDFuTMAsGA1UdDwQEAwIBhjAQBgkrBgEEAYI3FQEE
AwIBADBUBgNVHSAETTBLMEEGCisGAQQBgd55AQEwMzAxBggrBgEFBQcCARYlaHR0ccDovL3d5dy5o
ZWFsdGhzaWduLm9yZy9yZXBvc2l0b3J5LzAGBgRVHSAAMBkGCSsGAQQBgicUAgQMHgoAUwB1AGIA
QwBBMB8GA1UdIwQYMBaAFAtuk2JdyGpgwCgfurOve+HTcrF5MEAGA1UdHwQ5MDcwNaAzoDGGL2h0
dHA6Ly93d3cuaGVhbHRoc2lnbi5vcmcvcmVwb3NpdG9yeS9oZXNpY2EuY3JsMEsGCCsGAQUFBwEB
BD8wPTA7BggrBgEFBQcwAoYuaHR0cDovL3d3dy5oZWFsdGhzaWduLm9yZy9yZXBvc2l0b3J5L2hl
c2lyYS5jcnQwDQYJKoZIhvcNAQEFBQADggEBADJQ0tyrDH8xSLqSZpcVlZCQbV7LwzsTiUiMMNqv
yTwPlnmPSZnwUH9sNVOU1VGM0MxU6ZtiOBpJjNtX75oy7EqhXZcwyXp/qDCBGWNPQ1fpiS0eDKQu
uyPvaPmx0TP2ZyZlk0/M3K0nyoSFoFTKrquNHq/arHiAUza52B7PkC0imQspj2Kb74kg/WLJlF2w5
HCSHYlgQ0PgvWSmHPBSCGyECbksZHY5S5OZEqx/F652kAxpdIBDytYGgAJH377ceKl2pQVUA+7lN
MdjRYesz3CnFoBPtxs3rIr2MlrzAH5Z2N/mLQDd911+74R83JplRyJhXunYpNPkKatN3Npz8qE=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA1withRSA

Issuer CN:

AC HEALTHSIGN

Issuer OU:

Albereda num. 3-5. Atic. 17004 - GIRONA

Issuer O:

HEALTHSIGN SL – CIF B17944554

Issuer C:

ES

Subject CN:

COMT CA

Subject OU:

Via Imperi Roma n. 11 bis. 43003 - TARRAGONA

Subject O:

Col-legi Oficial de Metges de Tarragona – CIF Q4366001H

Subject C:

ES

Valid from:

Fri Apr 27 10:25:12 CEST 2007

Valid to:

Wed Apr 27 10:35:12 CEST 2022

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DA:E8:57:22:99:08:3F:8F:34:58:B7:27:AA:BA:47:26:4B:99:2C:F8:4C:2B:5C:8E:BC:95:C9:F8:04:BC:3B:75:07:55:C
7:CA:AB:58:CC:AE:90:DC:26:6B:D1:05:5A:4D:FE:AA:9F:06:3E:47:CF:B2:BF:BB:CC:9E:7C:0D:85:70:B7:81:DD:EC:73:6D:40:19:EE:39:28:A7:75:AE:34:E4:57:CA:01:E3:FF:AE:53:36:4C:03:9E:2B:75:97:21:9E:AF:D2:5
5:AB:ED:7D:2B:69:60:5C:29:AF:FE:8C:23:0B:33:63:DA:EB:ED:3E:DD:AA:A3:6A:0B:83:5D:76:05:95:73:CB:72:64:D0:F7:F4:1A:8E:13:6C:E1:1E:C3:66:71:11:10:DC:36:FA:40:D1:88:1C:30:41:EE:8A:AE:07:2B:C1:71:9A
:49:6C:A3:CA:22:94:5F:F3:75:24:88:22:94:67:8F:8C:93:84:4F:64:E1:1E:73:5C:A7:77:0D:53:F6:38:D7:1F:B3:B4:A4:5B:81:DA:FA:CE:3B:83:0C:A0:10:1E:DF:0A:BE:1A:B0:0C:92:50:76:C5:80:89:B7:41:B1:DB:7F:7B:44:F
7:F6:B8:7C:6E:0E:26:AF:CB:FA:FE:2B:A6:49:8D:52:09:F9:FE:D7:ED:3D:48:8F:B8:8E:B4:37:02:03:01:00:01
```


Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

A7:66:F5:29:2C:0F:C3:03:90:A5:98:72:29:96:05:B0:45:0C:5B:93

Certificate Policies

Policy OID: 1.3.6.1.4.1.28537.1.1

CPS pointer: http://www.healthsign.org/repository/

Policy OID: 2.5.29.32.0

Authority Key Identifier

0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79

CRL Distribution Points

http://www.healthsign.org/repository/hesica.crl

Authority Info Access	*http://www.healthsign.org/repository/hesica.crt*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*FC:6F:34:24:8C:BB:7D:A5:73:06:E6:0C:4A:4F:92:4A:39:2D:7F:F6:FC:23:E6:04:27:08:3D:E7:72:7C:9E:A9*

X509SubjectName

Subject CN:	*COMT CA*
Subject OU:	*Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*
Subject O:	*Col-legi Oficial de Metges de Tarragona – CIF Q4366001H*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

9.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.6.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Member Certificate issued by CA COMT CA*
Name	*[es]*	*Certificado de Colegiado Reconocido emitido por CA COMT CA*

Service digital identities

X509SubjectName

Subject CN:	*COMT CA*
Subject OU:	*Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*
Subject O:	*Col-legi Oficial de Metges de Tarragona – CIF Q4366001H*
Subject C:	*ES*

X509SKI

X509 SK I	*p2b1KSwPwwOQpZhyKZYFsEUMW5M=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*
Status Starting Time	*2015-11-30T23:00:00Z*

9.6.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Member Certificate issued by CA COMT CA*
Name	*[es]*	*Certificado de Colegiado Reconocido emitido por CA COMT CA*

Service digital identities

X509SubjectName

Subject CN:	*COMT CA*
Subject OU:	*Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*
Subject O:	*Col-legi Oficial de Metges de Tarragona – CIF Q4366001H*
Subject C:	*ES*

X509SKI

X509 SK I	*p2b1KSwPwwOQpZhyKZYFsEUMW5M=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2009-09-09T00:00:00Z*

10 - TSP: Infraestructuras y Servicios de Telecomunicaciones y Certificación SA

.

TSP Name

Name	*[en]*	*Infraestructuras y Servicios de Telecomunicaciones y Certificación SA*
Name	*[es]*	*Infraestructuras y Servicios de Telecomunicaciones y Certificación SA*
Name	*[ca]*	*Infraestructures i Serveis de Telecomunicacions i Certificació*
Name	*[en]*	*Instituto Valenciano de Finanzas*

TSP Trade Name

Name	*[en]*	*Agencia de Tecnología y Certificación Electrónica - ACCV*
Name	*[es]*	*Agencia de Tecnología y Certificación Electrónica - ACCV*
Name	*[en]*	*ACCV*
Name	*[es]*	*ACCV*
Name	*[en]*	*Generalitat Valenciana*
Name	*[es]*	*Generalitat Valenciana*
Name	*[en]*	*Institut Valenciá de Finances - IVF*
Name	*[es]*	*Institut Valenciá de Finances - IVF*
Name	*[en]*	*Instituto Valenciano de Finanzas*
Name	*[en]*	*VATES-A40573396*

PostalAddress

Street Address	*[en]*	*Pista de Ademuz S/N*
Locality	*[en]*	*Burjassot*
State Or Province	*[en]*	*Valencia*
Postal Code	*[en]*	*46100*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Pista de Ademuz S/N*

Locality	*[es]*	*Burjassot*
State Or Province	*[es]*	*Valencia*
Postal Code	*[es]*	*46100*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:accv@accv.es*
URI	*[en]*	*http://www.accv.es*

TSP Information URI

URI	*[en]*	*http://www.accv.es/quienes-somos/who-are-we*
URI	*[es]*	*http://www.accv.es*

10.1 - Service (withdrawn): Certificados Reconocidos emitidos por CA ACCV-CA2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por CA ACCV-CA2*
Name	*[en]*	*Qualified Certificates issued by ACCV-CA2*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*1146754895*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGdTCCBV2gAwIBAgIERFoXTzANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJFUzEfMB0GA1UE
ChMWR2VuZXJhbGl0YXQgVmFsZW5jaWFuYTEPMA0GA1UECxMGUEtJR1ZBMSewJQYDVQQDEx5Sb290
IENBIEdlbmVyYWxpdGF0IFZhbGVuY2lhbmEwHhcNMDYwNTA0MTUwMTM1WhcNMTYwNTAxMTUwMTM1
WjBSMREwDwYDVQQDEwhBQ0NWLUNBMjEPMA0GA1UECxMGUEtJR1ZBMR8wHQYDVQQKExZHZW5lcmFs
aXRhdCBWYWxlbmNpYW5hMQswCQYDVQQGEwJFUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBANu0lEp2zD/f5ypSi9rv2pgQtNn6k9l/d3raJ+ZSSdVP/H2YhXq+p5Y03raY5dklgcJVt4bn0O
RTpmZAIifpNlewKfn9RLgO9ZY474I8sRT06NscFIIr/CYJAtzzIkGiIQPi1CyRI+qf+ZUFDRfIm6usP
2t6I1XVIfkCwnf2pa37Wphf7x2ZOcpOtZalpeY/OJ7Jztj0buovdZVLtM2pg64dLui5We8bQaqyV
epHsbdRn9vr5IVw1L6+ZZcJC2iiQmFKSx1gjB1ca46UvWyIr8lDViWS74nPulhfv17mPcIN2CBjER
QbXziAGp1AQErUHMYgbzVMVHHX1ta95EIT9NJ+JvIsCAwEAAaOCAzswggM3MBIGA1UdEwEB/wQI
MAYBAf8CAQAwggI0BgNVHSAEggIrMIICJzCCAiMGCisGAQQBvIUCAQAwggITMIIB6AYIKwYBBQUH
AgIwggHaHoIB1gBBAHÚAdABvAHlAaQBkAGEAZAAgAGQAZQAgAEMAZQByAHQAaQBmAGkAYwBhAGMA
aQDzAG4AIABSAGEA7QB6ACAAZABlACAAbABhACAARwBlAG4AZQByAGEAbABpAHQAYQB0ACAAVgBh
AGwAZQBuAGMAaQBhAG4AYQAuA0ACgBMAGEAIABEAGUAYwBsAGEAcgBhAGMAaQDzAG4AIABkAGUA
IABQAHlAdQBjAHQAaQBjAGEAcwAgAGQAZQAgAEMAZQByAHQAaQBmAGkAYwBhAGMAaQDzAG4AIABx
AHUAZQAgAHIAaQBnAGUAIABlAGwAIABmAHÚAbgBjAGkAbwBuAGEAbQBpAGUAbgB0AG8AIABkAGUA
IABsAGEAIABwAHIAZQBzAGUAbgB0AGUAIABBAHÚAdABvAHIAaQBkAGEAZAAgAGQAZQAgAEMAZQBy
AHQAaQBmAGkAYwBhAGMAaQDzAG4AIABzAGUAIABlAG4AYwB1AGUAbgB0AHÍAYQAgAGÚAbgAgAGwA
YQAgAGQAaQByAGUAYwBjAGkAÓnBuACAAdnBlAG1AIABnAHQAdAIBwADoALwAvAHcAdwB3AC4AcABr
AGkALgBnAHYAYQAuAGUAcwAvAGMAcABzMCUGCCsGAQUFBwIBFhlodHRwOi8vd3d3LnBraS5ndmEu
ZXMvY3BzMDIGCCsGAQUFBwEBBCYwJDAiBggrBgEFBQcwAYYWaHR0cDovL29jc3AucGtpLmd2YS5l
czCBlQYDVR0jBIGNMIGKgBR7NdNA0hx4GWbvdBAo3D5PsngEKFspGowaDELMAkGA1UEBhMCRVMx
HzAdBgNVBAoTFkdlbmVyYWxpdGF0IFZhbGVuY2lhbmExDzANBgNVBAsTBlBlLSUdWQTEmMCUGA1UE
AxMeUm9vdCBDQSBHZW5lcmFsaXRhdCBWYWxlbmNpYW5hggQ7Re VoMB0GA1UdDgQWBBSzc00FpXlB
OsL0wFlo/2NDP7/jgTANBgkqhkiG9w0BAQUFAAOCAQEAD3YL1dnc7aPa3LoA Yon5INw/q7DYkyMX
gL3tGLh3Cw1E8uiaC3sZrbFZiY7kZ7duVUEix/XCiLAjpcaWCwz9l4eMEhJUi+mSG6FVQqQ6ILBS
qCYwIaKkPARy44bmZOhXPKj29jiGw6kgbPNvkDYH54h60TzkRZn/MO1mfb8uz2dOfoFj3Q5Avx/
+XatGXb4cBtKDOXmFsDmdGQK3Qn8+jeQPWzpvjotC0fcHCUNiHoo9XkDTZSc++6qe7nUQoSQsG
bk3psOl/BfwepaACucuBo8IMXZvdqD9zULh7czfj1xq0jUaZCPqR2SBpoVwwzNrVLXaGnYiFjNit
lPRFAA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Root CA Generalitat Valenciana*

Issuer OU: *PKIGVA*

Issuer O: *Generalitat Valenciana*

Issuer C: *ES*

Subject C: *ES*

Subject O: *Generalitat Valenciana*

Subject OU: *PKIGVA*

Subject CN: *ACCV-CA2*

Valid from: *Thu May 04 17:01:35 CEST 2006*

Valid to: *Sun May 01 17:01:35 CEST 2016*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DB:B4:12:9D:B3:0F:F7:F2:A5:28:BD:AE:FD:A9:81:0B:4D:9F:A9:3D:51:DD:EB:68:9F:99:49:27:55:3F:F1:F6:62:15:
EA:FA:9E:58:D3:7A:E2:A9:8E:5D:90:88:1C:25:5B:78:6E:7D:0E:45:3A:66:64:09:5F:A4:D9:5E:C0:A9:67:F5:12:E0:3B:D6:55:E3:BE:1F:F2:C4:53:D3:A3:6C:70:59:48:AF:F0:98:24:0B:6B:CC:99:06:7D:03:E2:D4:2C:91:7F:E
A:9F:F9:95:05:0D:17:E6:EA:EB:0F:DA:DE:88:D5:75:65:7E:40:B0:9D:FD:A9:6B:7E:D6:A6:10:BB:C7:66:4E:7A:93:AD:65:A2:29:79:8F:CE:27:B2:73:B6:3D:1B:BA:8B:DD:65:52:ED:33:6A:60:EB:87:4B:BA:2E:56:7B:C6:
D0:6A:AC:95:7A:91:EC:6D:D4:67:F6:FE:48:57:0D:4B:EB:E6:59:70:90:B6:8A:24:26:14:A4:B1:D6:08:C1:D5:C6:B8:E9:4B:D6:C8:8A:FC:94:35:62:59:2E:F8:9C:FB:A5:85:FB:F5:EE:63:DC:94:DD:82:06:31:11:40:8C:57:8A:
20:06:A7:50:10:12:B5:07:31:88:1B:CD:53:15:1C:75:F5:89:AF:79:12:54:FD:34:9F:89:BE:5B:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 1.3.6.1.4.1.8149.2.1.0*

*CPS text: [Autoridad de Certificación Raíz de la Generalitat Valenciana.
La Declaración de Prácticas de Certificación que rige el funcionamiento de la presente Autoridad de Certificación se encuentra en la dirección web http://www.pki.gva.es/cps]*

CPS pointer: http://www.pki.gva.es/cps

Authority Info Access *http://ocsp.pki.gva.es*

Authority Key Identifier *7B:35:D3:40:D2:1C:78:19:66:EF:74:10:28:DC:3E:4F:B2:78:04:FC*

Subject Key Identifier *B3:78:ED:05:A5:79:41:3A:C2:F4:C0:52:28:FF:63:43:3F:BF:E3:81*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AF:2A:96:31:00:E0:AB:38:18:E0:AD:5A:D4:38:22:1D:0C:B1:E8:6C:65:5E:5E:5A:9D:D3:1C:87:57:56:43:2C*

X509SubjectName

Subject C: *ES*

Subject O: *Generalitat Valenciana*

Subject OU: *PKIGVA*

Subject CN: *ACCV-CA2*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

10.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.16.2.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.17.2.0*

10.1.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.6.4.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.6.5.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

10.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

10.1.4 - History instance n.1 - Status: supervisionceased

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por CA ACCV-CA2

Name [en] Qualified Certificates issued by ACCV-CA2

Service digital identities

X509SubjectName

Subject C: ES

Subject O: Generalitat Valenciana

Subject OU: PKIGVA

Subject CN: ACCV-CA2

X509SKI

X509 SK I *s3jtBaV5QTrC9MBSKP9jQz+/44E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2016-05-01T00:00:00Z*

10.1.4.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.16.2.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.17.2.0*

10.1.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description

[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.7.1.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.6.4.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.6.5.0*

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

10.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Certificados Reconocidos emitidos por CA ACCV-CA2*

Name [en] *Qualified Certificates issued by ACCV-CA2*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *Generalitat Valenciana*

Subject OU: *PKIGVA*

Subject CN: *ACCV-CA2*

X509SKI

X509 SK I *s3jtBaV5QTrC9MBSKP9jQz+/44E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-03-16T00:00:00Z*

10.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.16.2.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.17.2.0

10.1.5.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.6.4.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.6.5.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

10.2 - Service (withdrawn): Qualified Certificates issued by CA GVA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by CA GVA*

Name [es] *Certificados Reconocidos emitidos por CA GVA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number:

999621763

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGgjCCBWgAwIBAgIEO5UEgzANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJFUzEtMB0GA1UE
ChMWR2VuZXJhbGl0YXQgVmFsZW5jaWFuYTEPMA0GA1UECxMGUEtJR1ZBMScwJQYDVQQDEx5Sb290
IENBIEdlbmVyYWxpdGF0IFZhbGVuYZlhbmEwHhcNMDEwOTA0MTY0MjQzWhcNMTEwOTAyMTY0MjQz
WjBPMQswCQYDVQQGEwJFUzEtMB0GA1UEChMWR2VuZXJhbGl0YXQgVmFsZW5jaWFuYTEPMA0GA1UE
CxMGUEtJR1ZBMQ4wDAYDVQQDEwVJQUIgWQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AOAP3NA1QQ9oRi8pqDsd3N9ZNvdQNVE9EYTrA++jPU7N32X8RfceXcEHfuVDupYeYjZX2ZpKjsF3
TfDst+Ub+axedcHXfvCX+U7QoFJ0OYdjgPjN95JhvrXrik2Rt8qW5IeL7J7FTSl6ZTRuakenl6Z4
Mz7T00lyjuXvu4nqSAM1a+bt85NtRWqUvaK9pdHPPQsVYj/Wprw/EJRMwq+WWIQ9KE+6DJiUuUW+
Fwx503nTQZaABRkk8aj+1z0FMU/prfj1iaP8r8yzirB3XwEubv/DUPlLFWM0w9IFv2lPqHruUJb/b
BkZorXu0ad51ZXPnwb7WgkdhIZ3pn2I2qnUYScCAwEAAaOCA0swggNIMBIGA1UdEwEB/wQIMAYB
Af8CAQAwDgYDVR0PAQH/BAQDAgEGMIICNAYDVR0gBIICKzCCAicwggIjBgorBgEEAb9VAgEAMIIC
EzCCAcegGCCsGAQUFBwICMIIB2h6CAdYAQQB1AHQAbwByAGkAZABhAGQAIABkAGUAIABDAGUAcgB0
AGkAZgBpAGMAYQBjAGkA8wBuACAAUgBhAO0AcgAgAGQAZQAgAGwAYQAgAEcAZQBuAGUAcgBhAGwA
aQB0AGEAdAAgAFYAYQBsAGUAbgBjAGkAYQBuAGEALgANAAoATAIBhACAARAIBlAGMAbAIBhAHIAYQBj
AGkA8wBuACAAZABlACAAUAByAOEAYwB0AGkAYwBhAHMAIABkAGUAIABDAGUAcgB0AGkAZgBpAGMA
YQBjAGkA8wBuACAAcQB1AGUAIAByAGkAZwBlACAAZQBsACAAZgB1AG4AYwBpAG8AbgBhAG0AaQBl
AG4AdABvACAAZABlACAAbABhACAAcAByAGUAcwBlAG4AdABlACAAQQB1AHQAbwByAGkAZABhAGQA
IABkAGUAIABDAGUAcgB0AGkAZgBpAGMAYQBjAGkA8wBuACAAcwBlACAAZQBuAGMAdQBlAG4AdABy
AGEAIABlAG4AIABsAGEAIABkAGkAcgBlAGMAYwBpAPMAbgAgAHcAZQBiACAAaAB0AHQAcAA6AC8A
LwB3AHcAdwAuAHAAawBpAC4AZwB2AGEALgBlAHMALwBjAHAAczAIBggrBgEFBQcCARYZaHR0cDov
L3d3dy5wa2kuZ3ZhLmVzL2NwczAyBggrBgEFBQcBAQQmMCQwIgYIKwYBBQUHMAGGFmh0dHA6Ly9v
Y3NsLnBraS5mdmFuZXMwgZUGA1UdIwSBjTCBioAUczXTQNIceBIm73QKNw+T7I4BPybhKRgMGgx
CzAJBgNVBAYTAkVTMR8wHQYDVQQKEwZHZW5lcmFsaXRhdCBWYWxlbmNpYW5hMQ8wDQYDVQQLEwZQ
S0lHVkExJzAlBgNVBAMTHUJvb3QgQ0EgR2VuZXJhbGl0YXQgVmFsZW5jaWFuYYIEO0XlaDAdBgNV
HQ4EFgQUc/UwDVPJya1yNHnHUWIIN1x9Xt90wDQYJKoZIhvcNAQEFBQADggEBAMJUkB2rHyI78DbC
RcpuTjjUh2AjPFxVqBGMYEGcAR39+tS2kveRV8FBXU/KpOJp8kXBWWDYwkR37MZQizxP+bpAyssgPLX
OXJYFo5IBbMicuPZK8LDAXymIquFsxw341/Mb+qWe6bXrVocfN7pqQxQSLba1xXKVJrwKgrwNT6p
ee+PIYT+GtREyPkGwXMMuAMX8nzsDnjFUjT+S3qrpb9AmTiLXZenAVyGTY8QueTBUzocj7kEZ1X
vVnJsMI5WeghsxbhEHtEjYIOKneJuXc4PWBtrjIIFBw7lrYZG/+MONEesGjQhfE2wIrtpPMmZtAaM
NzKC3DJMW7bCOCn+5v2GGZw=

-----END CERTIFICATE-----

Signature algorithm:

SHA1withRSA

Issuer CN:

Root CA Generalitat Valenciana

Issuer OU:

PKIGVA

Issuer O:

Generalitat Valenciana

Issuer C:

ES

Subject CN:

CAGVA

Subject OU:

PKIGVA

Subject O:

Generalitat Valenciana

Subject C:

ES

Valid from:

Tue Sep 04 18:42:43 CEST 2001

Valid to:

Fri Sep 02 18:42:43 CEST 2011

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E0:0F:DC:D0:35:40:6F:68:45:FF:29:A8:3B:1D:DC:DF:59:36:FD:10:35:51:3D:11:84:EB:03:EF:A3:3D:4E:CD:DF:65:FC:45:F7:1E:5D:E1:07:7E:E5:43:BA:96:1E:62:36:40:D9:9A:4A:8E:C1:77:4D:F0:EC:B7:E5:1B:F9:AC:5E:75:C1:D7:7E:F0:97:F9:4E:D0:A0:52:74:39:87:63:80:F8:CD:F7:92:61:BE:25:EB:8A:4D:91:B7:CA:96:E4:87:8B:EC:9E:C5:4D:29:7A:65:34:6E:6A:47:A7:97:A6:78:33:3E:D3:D3:49:72:8E:E5:EF:BB:89:EA:48:03:35:6B:E6:DF:F3:93:6D:45:6A:94:BD:A2:BD:A5:D1:CF:3D:0B:15:62:3F:D6:A6:BC:3F:10:94:4C:C2:AF:96:58:84:3D:28:4F:BA:0C:98:94:B9:45:BE:17:0C:79:D3:79:D3:41:96:80:05:19:24:F1:A8:FE:D7:3D:05:31:4A:6B:7E:3D:62:68:FF:2B:F3:2C:E2:AC:15:EB:C0:4B:9B:BF:F0:D4:3E:52:C5:58:CD:30:F4:81:6F:DA:53:EA:1E:BB:94:26:2F:DB:06:46:68:AD:7B:B4:69:DE:75:65:73:E7:C1:BE:D6:AA:47:62:25:F6:77:A6:8D:88:DA:AC:14:63:97:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Certificate Policies

Policy OID: 1.3.6.1.4.1.8149.2.1.0

*CPS text: [Autoridad de Certificación Raíz de la Generalitat Valenciana.
La Declaración de Prácticas de Certificación que rige el funcionamiento de la presente Autoridad de Certificación se encuentra en la dirección web http://www.pki.gva.es/cps]*

CPS pointer: http://www.pki.gva.es/cps

Authority Info Access

http://ocsp.pki.gva.es

Authority Key Identifier

7B:35:D3:40:D2:1C:78:19:66:EF:74:10:28:DC:3E:4F:B2:78:04:FC

Subject Key Identifier

71:4C:03:54:F2:72:6B:5C:8D:1E:71:D4:58:82:0D:D7:1F:57:B7:DD

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9D:AE:71:05:BD:9A:45:07:D2:78:21:01:FD:23:19:10:88:3E:22:27:26:47:0E:2D:98:33:3B:68:7F:9A:4F:63*

X509SubjectName

Subject CN: *CAGVA*

Subject OU: *PKIGVA*

Subject O: *Generalitat Valenciana*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

10.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.2.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name *[en]* *Qualified Certificates issued by CA GVA*

Name *[es]* *Certificados Reconocidos emitidos por CA GVA*

Service digital identities

X509SubjectName

Subject CN:	*CAGVA*
Subject OU:	*PKIGVA*
Subject O:	*Generalitat Valenciana*
Subject C:	*ES*

X509SKI

X509 SK I	*cUwDVPJya1yNHnHUWIIN1x9Xt90=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*
Status Starting Time	*2012-04-15T22:00:00Z*

10.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA GVA*
Name	*[es]*	*Certificados Reconocidos emitidos por CA GVA*

Service digital identities

X509SubjectName

Subject CN:	*CAGVA*
Subject OU:	*PKIGVA*
Subject O:	*Generalitat Valenciana*
Subject C:	*ES*

X509SKI

X509 SK I	*cUwDVPJya1yNHnHUWIIN1x9Xt90=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2005-11-03T00:00:00Z*

10.3 - Service (withdrawn): Qualified Certificates issued by ACCV-CA1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by ACCV-CA1*

Name *[es]* *Certificados Reconocidos emitidos por ACCV-CA1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1146745616*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGQTCCBSmgAwIBAgIERFnzEDANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJFUzEfMB0GA1UE
ChMWR2VuZXJhbGl0YXQgVmFsZW5jaWFuYTEPMA0GA1UECxMGUEtJR1ZBMScwJQYDVQQDEx5Sb290
IENBIEdlbmVyYWxpdGF0IFZhbGVuY2lhbmEwHhcNMDYwNTA0MTIyNjU2WhcNMTYwNTAxMTIyNjU2
WjBSMREwDwYDVQQDEwhBQ0NWLUNBMTEPMA0GA1UECxMGUEtJR1ZBMR8wHQYDVQQKExZHZW5lcmFs
aXRhdCBWYWxlbmNpYW5hMQswCQYDVQQGEwJFUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBALkHCgPv1j0O3AKHrwLszF/0wXpx9WL2TptsuiAbOJNNwa0mV4IKyvyNhm2tW6dX+Kf8wtP
DOEEuK0KcZ9QSQfh2qdq7EiybpIG7NdxqOsioWzqY/8YUJjeIrl46l1TRs8OJcqvSUiPcrdb7
mNngNkddd CGCmSx5SDe6U3XKItc0tfiqWqKPLr8F1w14RmVXmmcdqKK1jRak+btDTBicIN//0PAR
RTF1XRVRJ7srAv7J75jz+2nWv+7lkDCY4fyJtD7WPNEe5ta4qxjnMumMqSj+wOldTSACY7oEAZkP
zMWR4U4ZT9dku0Pdboe9ny3IlkQYLJEUWeiQ34XMunECAwEAAaOCAwcwggMDMBIGA1UdEwEB/wQI
MAYBAf8CAQAwggf08gNVHSAEggfMIICJzCCAiMGCisGAQQBs1UCAQAwggITMIIB6AYIKwYBBQUH
AgfwggHaHoIB1gBBAHUAdABvAHIAaQBkAGEAZAAgAGQAZQAgAEMAZQByAHQAaQBmAGkAYwBhAGMA
aQDzAG4AIABSAGEA7QB6ACAAZABlACAAbABhACAARwBlAG4AZQByAGEAbABpAHQAYQB0ACAAVgBh
AGwAZQBuAGMAaQBhAG4AYQAuAA0ACgBMAGEAIABEAGUAYwBsAGEAcgBhAGMAaQDzAG4AIABkAGUA
IABQAHIAaQBjAHQAaQBjAGEAcwAgAGQAZQAgAEMAZQByAHQAaQBmAGkAYwBhAGMAaQDzAG4AIABx
AHUAZQAgAHIAaQBnAGUAIABIAGwAIABmAHUAbgBjAGkAbwBuAGEADQBpAGUAbgB0AG8AIABkAGUA
IABsAGEAIABwAHIAZQBzAGUAbgB0AGUAIABBAHUAdABvAHIAaQBkAGEAZAAgAGQAZQAgAEMAZQBy
AHQAaQBmAGkAYwBhAGMAaQDzAG4AIABzAGUAIABIAG4AYwB1AGUAbgB0AHIAYQAgAGUAbgAgAGwA
YQAgAGQAaQBvAGUAYwBjAGkA8wBuACAAdwBlAGIAIABoAHQAdABwADoALwAvAHcAdwB3AC4AcABr
AGkAL gBnAHYAYQAuAGUAcwAvAGMAcABzMCUGCCsGAQUFBwIBFhlodHRwOi8vd3LnBraS5ndmEu
ZXMvY3BzMIGVBgNVHSMEgY0wgYqAFHs100DSHHgZZu90ECjcPk+ycAT8oWykajBoMQswCQYDVQQG
EwJFUzEfMB0GA1UEChMWR2VuZXJhbGl0YXQgVmFsZW5jaWFuYTEPMA0GA1UECxMGUEtJR1ZBMScw
JQYDVQQDEx5Sb290IENBIEdlbmVyYWxpdGF0IFZhbGVuY2lhbmGCBDtF5WgwHQYDVR00BBYEFBuQ
hevMw/l02Zlvqxt80QTDIyiRSMA0GCSqGSIb3DQEBBQUAA4IBAQBCPva/OGwpCDmtgB1KWN3NrWNS
F6d4CmGuhrUhZF/VojcLIWq5YQMmHdJLem/r4+mlddcF23XaXQf4z675lV1RrnZMij56eNbbrVkU
eP3hvSr37C3SIBPlC/Z/hCzceuZrWTdjL VRmAmV8BEaR3lONkJnyHgFNjwFAslct37lUH20mdRbB
pnzhImR+t44E8tfpqxA/AQMlrgrRLuVG5m2izrj8LKF5G2y2J8aYdeLNsAcni1/j342shHi1XiqkF
g0DXoeCxcx6dZcAxGgDFwwx+o6QU7unl5KFKuOkE3SSbNG5nCrltB9DrcTMLlk3EhaFiO48Caif5
MA08VrkL07bN
-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Root CA Generalitat Valenciana*

Issuer OU: *PKIGVA*

Issuer O: *Generalitat Valenciana*

Issuer C: *ES*

Subject C: *ES*

Subject O: *Generalitat Valenciana*

Subject OU: *PKIGVA*

Subject CN: *ACCV-CA1*

Valid from: *Thu May 04 14:26:56 CEST 2006*

Valid to: *Sun May 01 14:26:56 CEST 2016*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:07:0A:03:EF:D6:3D:0E:DC:02:87:AF:02:EC:CC:5F:F4:C1:7A:71:F5:65:8B:D9:3B:69:B2:E8:80:6C:E2:4D:37:06:B4:99:5E:08:2B:2C:8D:86:6D:A2:B5:6E:9D:5F:E2:9F:F3:07:CF:0C:E1:04:B8:AD:0A:79:9F:6D:41:24:1F:87:6A:9D:AB:B1:2D:FF:26:E9:24:6E:CD:77:1A:8E:B2:2A:16:B2:BA:98:FF:C6:09:26:37:88:CF:8E:88:D5:34:6C:44:EF:C9:72:AB:D2:52:23:DC:AD:D8:7B:9B:C3:60:36:47:5D:74:21:82:99:2C:79:48:37:BA:53:75:CA:22:D7:34:B5:F6:AA:5A:A2:8F:2E:BF:05:D7:0D:78:46:65:57:9A:67:1D:A8:A2:B5:8D:16:A4:F9:BB:43:4C:17:DC:88:DF:FF:D0:F0:11:45:31:75:5D:15:51:27:BB:2B:02:FE:C9:EE:C8:F3:FB:69:D6:BF:EE:E5:90:30:98:E1:FC:89:B4:3E:D6:3C:D1:1E:E6:D6:B8:AB:18:E7:32:E9:8C:A9:28:FE:C0:E2:1D:4D:20:02:63:BA:04:01:99:0F:CC:C5:91:E1:4E:19:4F:D7:64:BB:43:DD:6E:87:BD:9F:2D:E5:7E:44:18:2C:91:14:59:E8:90:DF:85:CC:BA:71:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 1.3.6.1.4.1.8149.2.1.0*

*CPS text: [Autoridad de Certificación Raíz de la Generalitat Valenciana.
La Declaración de Prácticas de Certificación que rige el funcionamiento de la presente Autoridad de Certificación se encuentra en la dirección web http://www.pki.gva.es/cps]*

CPS pointer: http://www.pki.gva.es/cps

Authority Key Identifier *7B:35:D3:40:D2:1C:78:19:66:EF:74:10:28:DC:3E:4F:B2:78:04:FC*

Subject Key Identifier *1B:90:85:EB:CC:C2:5D:36:64:9B:EA:C6:24:74:41:30:C9:CA:24:52*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C7:D8:33:48:A3:0A:A6:7A:79:C7:20:38:D1:EF:E5:33:18:89:E6:4D:A1:47:E2:7A:1D:8F:FE:47:AE:8C:BE:29*

X509SubjectName

Subject C: *ES*

Subject O: *Generalitat Valenciana*

Subject OU: *PKIGVA*

Subject CN: *ACCV-CA1*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

10.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.10.1.0*

10.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.3.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ACCV-CA1*
Name	*[es]*	*Certificados Reconocidos emitidos por ACCV-CA1*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject O:	*Generalitat Valenciana*
Subject OU:	*PKIGVA*
Subject CN:	*ACCV-CA1*

X509SKI

X509 SK I	*G5CF68zCXTZkm+rGJHRBMMnKJFI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2016-05-01T00:00:00Z*

10.3.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.10.1.0*

10.3.3.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.10.1.0*

10.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ACCV-CA1*

Name *[es]* *Certificados Reconocidos emititdos por ACCV-CA1*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *Generalitat Valenciana*

Subject OU: *PKIGVA*

Subject CN: *ACCV-CA1*

X509SKI

X509 SK I *G5CF68zCXTZkm+rGJHRBMMnKJFI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-03-16T00:00:00Z*

10.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.10.1.0*

10.3.4.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description

[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.10.1.0*

10.4 - Service (granted): Qualified Certificates issued by ACCVCA-110

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by ACCVCA-110*

Name *[es]* *Certificados Reconocidos emitidos por ACCVCA-110*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2367878857421211669*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHeTCCBWGgAwIBAgIINxIRne/yBUwDQYJKoZIhvcNAQEFBQAwQjESMBAGA1UEAwwJQUNDVUB
SVoxMRAwDgYDVQQLDAdQS0lBQ0NWMQ0wCwYDVQQKDARBQ0NWMQswCQYDVQQGEwJFUzAeFw0xMTEw
MTMxMTIyMDRaFw0yNjEyMzEyMzU5MDBaMEMxEzARBgNVBAMMCkFDQ1ZDQS0xMTAxEDAOBgNVBAsM
B1BLSUFDQ1YxDTALBgNVBAoMBEFDQ1YxCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAoFlVLyy+mK29v/sQZfjQLLkr3gEHI1cA7Ev0mJkOjx5jkpk7xp7NbROz/EM5
VVxZVi+mo8Wdqc8Qzrgm4XQNa0la4LC8f4boxdmLND0zCnfGNxtl15tPdHIqZ7k9u+YkyIL5
MX5VNbWl/TgMjxUHzaORYKPbSMRIAQSdJ1b7OU0PNa7p+WoF2XqbUzMdR0qw03tsyBvvRXgTFkIKi
jzHDA5cemDfSdZNP7t6LOxu0JxKDIqgyMFH88FqdeJd8uYVWpBpohlZ0Gt7r3K9b6jNzuVAtWlk
l4cByw1n5wmMSgxPxX6BtQrFUrvilrgdzDc/8b4IBqFzINjX/P9nErJdd4aQsn62uEomZ8PUwnQ6
xhkMSqFjKDaqKUKjlSCv+PQoBA60Wulhgoxkw CIIYS5V0uciAFams8YJt3U0ZNtzR4g+JUIPjn7
Vboi8OW5YKyxentQ+kDRN6gCQc8Oysx8NJ0wZnyt8MFzb/4OlzsO3vjSl8QEk9F0QF9+3ycmFz6d
BLYQgsZDDyK28DkJbIvwtDevB0S2QrabM3sxyKBImG7rNMm7ZyxpvX9vPXz1eGgxhJ/pTCZMBe2/
ygFRLjoHEJhkSJCiooCFluUccYlPq1PugwVeIzpZZOVZvwPV0SKAJV+TdvZVW0jF7zs8EoVJpW
9z7BiD3GumxZSckCAwEAAaOCAnAwggJsMC8GCCsGAQUFBwEBBCMwITAfBggrBgEFBQcwAYYTaHR0
cDovL29jc3AuYWNjdi5lczAdBgNVHQ4EFgQUkIKuRm1bvb6FwbNhR6j19mTwA4wDwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMEGDAWgBTSb7Tj3zcnk1X2VuqB5TbMjB4/vTCCAX8GA1UdIASCAXYwggFy
MIIBbgYEVR0gADCCAWQwggFuBggrBgEFBQcCAjCCASAeggEcAEEAdQB0AG8AcgBpAGQAYQBkCACAA
ZABlACAAQwBlAHIAdABpAGYAaQBjAGEAYwBpAPMAbgAgAEEAbgB0AGUAcgBtAGUAZABpAGEAIABk
AGUAIABsAGEAIABBAEMAQwBWACAAKABBAGcAZQBuAGMAaQBhACAAZABlACAAYABlAGMAbgBvAGwA
bwBnAO0AYQAgAHkAIABDAGUAcgB0AGkAZgBpAGMAYQBjAGkA8wBuACAARQBsAGUAYwB0AHIA8wBu
AGkAYwBhACwAIABDAEkARgAgAFEANAA2ADAAMQAxADUANgBFACkALgAgAEMAUABTACAAZQBuACAA
aAB0AHQAcAA6AC8ALwB3AHcAdwAuAGEAYwBjAHYALgBlAHMwMAYIKwYBBQUHAgEWJGh0dHA6Ly93
dXcuYWNjdi5lcy9sZWdpc2xhYl2hb9lLmh0b TBVBgNVHR8E TjBMMEIggSKBGhkR0dHRwOi8vd2d3
LmFjY3YuZXMvZmlsZWFkbWluL0FyY2hpdm9zL2NlcnRpZmljYWRvcy9yYWl6YWNjdjFtZGVyLmNy
bDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQEFBQADggIBAFCFt2jwrV487rm4tE+VWNX5E6jw
D32AXdEw6aDm1A2P4HYNMaQea88s7EyL4t2WImL1+B6Obrwmvl D1zbuja852KPQ92IUo00cBH0k1a
gonU/E72c4pHAHu36qZCYiGybvAI8A3wlm5+ow23zkLjLqfdAFA0Lrh16Sw3PImMC9L W69CnzU
14XBWtcmaqqqT1aJvoWUufk4703FJOZ+u6l+6l+VsR5IbFIbMOufhxTSVKyeIt7tpMFMAEK/mkbD
8SmWuLGymTtQUqj5pmBPmyZM1d0AvY4Dn9Fw6SOCw+YdkjnAxx5B9SnXBfphA3yMVob26WuWQxd0
Oz+ZuyLN4t5jcjl1UdH3wqjuS/UBBnTywVTyjxYB7HYT78yk0zTCNnCBmRlxL /fKzN2yRAr4/NU
SiltejMVQt6OtiSdalbwK16mvWlxAKZgP8ZthZ2hsnFC3EPvpt0P9dL A/O+F+vVt4/1vmMfQnx1
tudM4vUA7ul/KOYzfLmbnRojt8seiPGJrfLgvs4lXJXL65YMp9F0N/HH+lMZR9SgzyrRPb6V+eUY1
u4r9Cn+cC384CCugUgH4iKEKhW8Qe569eJzpjeQYE6qvCDFGfw8BCRN6Yq10W3zh2zbZ0mVtkRIQ
FX5aGAvZUMKRJ1PUDOd2apAeux4NhyH+FPbX0qU4r7ytR8j

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *ES*

Issuer O: *ACCV*

Issuer OU: *PKIACCV*

Issuer CN: *ACCVRAIZ1*

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-110*

Valid from: *Thu Oct 13 13:22:04 CEST 2011*

Valid to: *Fri Jan 01 00:59:00 CET 2027*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A0:75:4B:CB:2F:A6:88:2D:BD:BF:FB:10:65:F8:D0:2C:B9:2B:DE:01:07:23:57:00:EC:4B:F4:98:99:0E:8F:1E:63:92:9
9:3B:C6:9E:CD:6D:13:B3:FC:43:39:55:5C:59:56:2F:A6:A3:C5:AD:92:97:3C:43:3A:E0:9B:85:D0:35:A2:74:21:A2:38:2C:2F:1F:E1:BA:22:C7:49:8B:34:3D:33:0A:72:06:37:1B:62:D7:99:CF:E0:78:AA:67:B9:3D:BB:E6:24:C
A:52:F9:31:7E:55:35:B5:A5:FD:38:0C:8F:15:07:CD:A3:91:60:A3:DB:48:C4:65:01:04:9D:D5:BE:CE:53:43:CD:6B:BA:7E:5A:81:76:5E:A6:D4:CC:C7:51:D2:AC:34:DE:DB:32:06:FB:D1:5E:04:C5:90:82:A2:8F:31:C3:03:97:
1E:98:37:F1:75:93:4F:EE:DE:8B:3B:1B:B4:27:12:83:22:A8:2F:30:51:FC:F0:5A:9D:78:97:7C:B9:85:56:A4:1A:68:84:89:59:D0:6B:7B:AF:72:BD:6F:A8:CD:CE:E5:40:B5:69:64:97:87:01:CB:0D:67:E7:09:8C:4A:0C:4F:C5:7
E:81:B5:0A:C5:52:BB:E2:96:B8:1D:CC:37:3F:F1:BE:08:06:A1:73:20:D8:D7:FC:FF:67:12:B2:5D:77:86:90:B2:7E:B6:B8:4A:26:67:C3:D4:C2:74:3A:C6:19:0C:4A:A1:63:28:3A:AA:29:42:A3:97:90:AF:F8:F4:28:04:0E:B4:5
B:B:02:21:82:8C:64:C9:2D:48:62:2E:55:D2:E7:22:00:56:A6:B3:C6:09:8B:75:34:FD:93:6D:B5:1E:20:F8:95:25:3E:39:FB:55:BA:22:F0:E5:B9:60:AC:B1:7A:7B:50:FA:40:D1:37:A8:02:41:CF:0E:CA:CC:7C:34:9D:30:66:7C:AD
:10:C1:73:6F:FE:0E:97:3B:0E:DE:F8:D2:97:C4:04:93:D1:74:40:5F:7E:DF:27:26:17:3E:9D:04:B6:10:82:C6:43:0F:22:B6:F0:39:09:6C:8B:F0:B4:37:AF:07:44:B6:42:B6:9B:33:7B:31:C8:A0:48:98:6E:EB:34:C9:BB:67:2C:69:
BD:7F:6F:3D:7C:F5:78:68:31:84:9F:E9:4C:26:4C:05:ED:BF:CA:01:51:2E:3A:07:10:98:64:48:90:A2:A2:80:85:96:E5:1C:72:D6:25:3E:AD:4F:BA:0C:15:78:8C:E9:65:93:95:66:FC:0F:57:44:8A:02:55:7E:4D:D7:6F:65:55:B4:
8C:5E:F3:8B:C1:28:54:9A:56:F7:3E:C1:88:3D:C6:BA:6C:59:49:C9:02:03:01:00:01
```


Authority Info Access *http://ocsp.accv.es*

Subject Key Identifier *92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E*

Basic Constraints

IsCA: true

Authority Key Identifier

D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]

CPS pointer: http://www.accv.es/legislacion_c.htm

CRL Distribution Points

http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

13:45:C2:D3:9A:E4:B6:5C:CA:71:E8:8E:9A:2B:29:C7:1D:C9:13:F9:52:E9:35:A8:12:B0:04:DB:A7:AE:79:57

Certificate fields details

Version:

3

Serial Number:

3707946637220933198

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHkjCCBXqgAwIBAgIIM3VF0i2obk4wDQYJKoZIhvcNAQELBQAwQjESMBAGA1UEAwwJQUNDVlJB
SVoxMRAwDgYDVQQLDAdQS0lBQ0NWMQ0wCwYDVQQKDARBQ0NWMQswCQYDVQQGEwJFUzAeFw0xNTA1
MDcxMjI1MzIaFw0yNjEyMzEyMzU5MDBaMEMxEzARBgNVBAMMCkFDQ1ZDQS0xMTAxEDAOBgNVBAsM
B1BLSUFDQ1YxDTALBgNVBAoMBEFDQ1YxCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAoHVLyy+miC29v/sQZfjQLLkr3gEHI1cA7Ev0mJkOjx5jkpk7xp7NbROz/EM5
VVxZV+mo8Wdqpc8Qzrgm4XQNa0Ial4LCSf9bnxt0mLND0zCnIGNxtt15tPHfagZ7k9u+YkylL5
MX5VNbWl/TgMjxUHzaORYKPbSMRIAQSd1b7OU0PNa7p+WoF2XqbUzMdR0lqw03tsyBvvRXgTFkIKi
jzHDA5cemDfSdZNP7t6LOxu0JxKDJqgyMFH88FqdeJd8uYVWpBpohlIZ0Gt7t3K9b6jNzuVAtWlk
l4cByw1n5wmMSgxPcX6BtQrFUrvilrgdzDc/8b4IBqFzINjX/P9nEzJdd4aQsn62uEomZ8PUwnQ6
xhkMSqEjKDqgKUKjI5Cv+PQoBA60WwIbgoxkwCUYy5V0uciAFams8YJt3U0ZNtzR4g+JUlPjn7
Vboi8OW5YKyxentQ+kDRN6gCQc8Oysx8NJ0wZnyt8MFzb/4OlzsO3vjSl8QEk9F0QF9+3ycmFz6d
BLYQgsZDDyK28DlcJbIvwtDcvB0S2QrabM3sxyKBImG7rNMm7ZyxpvX9vPXz1eGgxhJ/pTCZMBe2/
ygFR1joHEJhkSJCiooCFluUccrYlPq1PugwVeIzpZZOVZvwPV0SKAJV+TddvZVW0jF7zs8EoVJpW
9z7BiD3GumxZSckCAwEAAaOCAnkwggKFMC3GCCsGAQUFBwEBBCMwITAfBggrBgEFBQcwAYYTaHR0
cDovL29jc3AuYWNjdi5lczAdBgNVHQ4EFgQUklKuRm1bvb6FwbNhR6j/t9mTwA4wDwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMEGDAWgBTSb7Tj3zcnk1X2VuqB5TbMjB4/vTCCAX8GA1UdIASCAXYwggFy
MIIBbgYEVR0gADCCAWQwggFuBggrBgEFBQcCAjCCASAeggEcAEEAdQB0AG8AcgBpAGQAYQBkACAA
ZABlACAAQwBlAHIAdAAgAGYAaQBjAGEAYwBpAPMAbgAgAEkAbgB0AGUAcgBtAGUAZABpAGEAIABk
AGUAIABsAGEAIABBAEMAQwBWACAAKABBAGcAZQBuAGMAaQBhACAAZABlACAAVABlAGMAbgBvAGwA
bwBnAO00AYQAgAHkAIABDAGUAcgB0AGkAZgBpAGMAYQBjAGkA8wBuACAARQBsAGUAYwB0AHlA8wBu
AGkAYwBhACwAIABDAEkARgAgAFEANAA2ADAAMQAxADUANgBFACkALgAgAEMAUABTACAAZQBuACAA
aAB0AHQAcAA6AC8ALwB3AHcAdwAuAGEAYwBjAHYALgBlAHMwMAYIKwYBBQUHAgEWJGh0dHA6Ly93
dXcuYWNjdi5lcy9sZWdpc2xhY2lvb9yLmh0bTBVBgNVHR8ETjBMMEggSKBGhkRodHRwOi8vdXd3
LmFjY3YuZXMvZmlsZWFkbWluL0FyY2hpdm9zL2NlcnRpZmljYWRvcy9yYWl6YWNjdjFIZGVyLmNy
bDAOBgNVHQ8BAf8EBAMCAQYwFwYDVR0RBBAwDoEMYWNjdkBbY2N2LmVzMA0GCSqGSIb3DQEBCwUA
A4ICAQA8URqZ+fk3JU/4/gkAdB7/XmRJ+la14KCe9GPl0vVVLThvCNrqkn3faW6I2VOBG72XsFst
II34VoY s6vQH+Qu/lCNbpjllxWRV6Do1Fr1o1ogKy2LK6TYUCmHudu99Fimf5TU1Lk/qCqpcROcAi
RA89X1aAOgRmETA8KqTN5xf08Vns7WOFLlDmCdikh+758TiqUKEfjytaKp41C3+0hEmQ/GYvzXV7
93N/Irwb4w6GMIIyr6YPiMRo9QzX604Ap0TI0RjxLXomnyNOz5jJWtxsxtbmsRrEcG/RT9OnKY
eYAiZQAV9oem+8hMzo9gwbSsxNXu7vQtBD9uIVwxc7GIlNuQ0y9iTIS2r0xxUoBIXD+X7V7848
f7Y/iQ429atAjB1PgLuESG9t+WDU4KYGYkuhberbYCDaVC90JCT9c2BzqZSkPCx0lWdpS6rUq0
shU2049yY5yMprjTua0FAflsv4H6fcam1plZQLHmO4q5lZKfenCCNjgPnYWh8gYPCWZdhDuGfnLo
BTRhhQqNkV0KC8lsF+nkYGrt+9jWLMhhcZJSTLvYhQguZa69j/cu4/JhbnoyCXiKiyocXD1mZYKX
wshHNga5f5XhDAWUEP72+DVNjSz/zc8dreVDSwc4m2/zBpPzvy4UB2uotlnJjpdeauVu/w46y9nn
eQXxRQ==

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer C:

ES

Issuer O:

ACCV

Issuer OU:

PKIACCV

Issuer CN:

ACCVRAIZ1

Subject C:

ES

Subject O:

ACCV

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-110*

Valid from: *Thu May 07 14:25:39 CEST 2015*

Valid to: *Fri Jan 01 00:59:00 CET 2027*

Public Key:

*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A0:75:4B:CB:2F:A6:88:2D:BD:BF:FB:10:65:F8:D0:2C:B9:2B:DE:01:07:23:57:00:EC:4B:F4:98:99:0E:8F:1E:63:92:9
9:3B:C6:9E:CD:6D:13:B3:FC:43:39:55:5C:59:56:2F:A6:A3:C5:AD:92:97:3C:43:3A:E0:9B:85:D0:35:A2:74:21:A2:38:2C:2F:1F:E1:BA:22:C7:49:8B:34:3D:33:0A:72:06:37:1B:62:D7:99:CF:E0:78:AA:67:B9:3D:BB:E6:24:C
A:52:F9:31:7E:55:35:B5:A5:FD:38:0C:8F:15:07:CD:A3:91:60:A3:DB:48:C4:65:01:04:9D:D5:BE:CE:53:43:CD:6B:BA:7E:5A:81:76:5E:A6:D4:CC:C7:51:D2:AC:34:DE:DB:32:06:FB:D1:5E:04:C5:90:82:A2:8F:31:C3:03:97:
1E:98:37:F1:75:93:4F:EE:DE:8B:3B:1B:B4:27:12:83:22:A8:2F:30:51:FC:F0:5A:9D:78:97:7C:B9:85:56:A4:1A:68:84:89:59:D0:6B:7B:AF:72:BD:6F:A8:CD:CE:E5:40:B5:69:64:97:87:01:CB:0D:67:E7:09:8C:4A:0C:4F:C5:7
E:81:B5:0A:C5:52:BB:E2:96:B8:1D:CC:37:3F:F1:BE:08:06:A1:73:20:D8:D7:FC:FF:67:12:B2:5D:77:86:90:B2:7E:B6:B8:4A:26:67:C3:D4:C2:74:3A:C6:19:0C:4A:A1:63:28:3A:AA:29:42:A3:97:90:AF:F8:F4:28:04:0E:B4:5
B:02:21:82:8C:64:C0:2D:48:62:2E:55:D2:E7:22:00:56:A6:B3:C6:09:8B:75:34:FD:93:6D:B5:1E:20:F8:95:25:3E:39:FB:55:BA:22:F0:E5:B9:60:AC:B1:7A:7B:50:FA:40:D1:37:A8:02:41:CF:0E:CA:CC:7C:34:9D:30:66:7C:AD
:F0:C1:73:6F:FE:0E:97:3B:0E:DE:F8:D2:97:C4:04:93:D1:74:40:5F:7E:DF:27:26:17:3E:9D:04:B6:10:82:C6:43:0F:22:B6:F0:39:09:6C:8B:F0:B4:37:AF:07:44:B6:42:B6:9B:33:7B:31:C8:A0:48:98:6E:EB:34:C9:BB:67:2C:69:
BD:7F:6F:3D:7C:F5:78:68:31:84:9F:E9:4C:26:4C:05:ED:BF:CA:01:51:2E:3A:07:10:98:64:48:90:A2:A2:80:85:96:E5:1C:72:D6:25:3E:AD:4F:BA:0C:15:78:8C:E9:65:93:95:66:FC:0F:57:44:8A:02:55:7E:4D:D7:6F:65:55:B4:
8C:5E:F3:8B:C1:28:54:9A:56:F7:3E:C1:88:3D:C6:BA:6C:59:49:C9:02:03:01:00:01*

Authority Info Access *http://ocsp.accv.es*

Subject Key Identifier *92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E*

Basic Constraints *IsCA: true*

Authority Key Identifier *D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]

CPS pointer: http://www.accv.es/legislacion_c.htm

CRL Distribution Points *http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl*

Subject Alternative Name *accv@accv.es*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E9:32:7A:34:7C:BE:1C:B9:4C:DC:9A:A5:4C:B3:1B:6E:43:D6:89:68:D1:7D:09:CE:32:6A:09:1B:FC:2F:0B:11*

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-110*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time *2018-01-16T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

10.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.10.2.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.22.1.0*

10.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

10.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ACCVCA-110*

Name *[es]* *Certificados Reconocidos emitidos por ACCVCA-110*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-110*

X509SKI

X509 SK I *klKuRm1bvb6FwbNhR6j/t9mTwA4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

10.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.10.2.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.22.1.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.10.3.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.22.2.0*

10.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ACCVCA-110*
Name	*[es]*	*Certificados Reconocidos emitidos por ACCVCA-110*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject O:	*ACCV*
Subject OU:	*PKIACCV*
Subject CN:	*ACCVCA-110*

X509SKI

X509 SK I	*klKuRm1bvb6FwbNhR6j/t9mTwA4=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2012-04-15T22:00:00Z*

10.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.10.2.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.22.1.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.10.3.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.22.2.0*

10.4.4.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.10.2.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.22.1.0*

10.5 - Service (granted): Qualified Certificates issued by ACCVCA-120

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by ACCVCA-120*
Name	*[es]*	*Certificados Reconocidos emitidos por ACCVCA-120*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7242567391183044774*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHkjCCBXqgAwIBAgIIZILEq2VLAKYwDQYJKoZIhvcNAQEFBQAwQjESMBAGA1UEAwwJQUNDVlJB
SVoxMRAwDgYDVQQLDAdQSlBlQ0NlMQ0wCwYDVQQKDARBQ0NlMQswCQYDVQQGEwJFUzAeFw0xMTEw
MTMxNDU1MDRaFw0yNEyMzEyMzUzMDBaMEMxEzARBgNVBAMMCkFDQ1ZDQS0xMjAxEDAOBgNVBAsM
B1BLSUFDQ1YxDTALBgNVBAoMBEFDQ1YxCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAmwYjFx7SZmarLj0+7DqdJn6qt5EwPpgXxnEzzFfOSQrSm6yIgIAIbVTEznl9
a5m/ydNAxggVGKNA+hNMFCagFSSP6nJ8bZ4SZbILpZ6cgUoXDV+Jy0FgW7sILPPh3233OtevxSi
wGEtipJBYZVP+qYMFEpedkLRI2HzF0XVrmS9YlWOzK7yh2+d4CqPCIX1W0uGeBK21skABXEXeRg
ZDr1USkmLRZAoG5NZB6XPcVdudBvIe3zO2nFPlYeDMsRSOBFwOp0L7tcEZ1dQ2u/uhq3UlGesWt
shn//sQDC8K7TX9whlRkw6Qx5V8TcO5xQNJaxBQnsNBw41TBX4sglwzF50wfA2Xn0PS4GhT0ms/
ijeqIh1ZP7eBKc4psMNJZtzhjdUCeK+WbZRDqK78Gv9K995oxFEDmR9Kyb5jDHgGV8qRdiup5g0t
anMSg2tU5RxGizjvdGUUDgAmvJfBuCMv15rLsz8c4zYxNDbNHRfET6TtxEZtLKTwGL3IrXgXANXL
FWSQzTw5EgBwueCWMZDIlv4x16oeX5G7QcrKrQS8DCdWhGlhDMVJOcBkkLJtRjKitmYiTIoRiF
aRt4S4+L+004rHlcbr9Ec76HbSmBYsmulfik8nSPDGnv0LOorMhaXdcn6c5RZpH008lv6fN5wpLe
EkQuzGjATLTFbo8CAwEAAaOCAokwggKFMC8GCCsGAQUFBwEBBCMwITAfBggrBgEFBQcwAYYTaHR0
cDovL29jc3Aa YWNjdc5kczAdBgNVHQ4EFgQU6fECbytmP8FE2KH1EgBQggXy+UwIwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMEGDAWgBTSh7Tj3zcnk1X2VuqB5TbMjB4/vTCCAX8GA1UdIASCAXYwggFy
MIIBbgYEVR0gADCCAWQwggFuBggrBgEFBQcCAjCCASAeggEcAEEAdQB0AG8AcgBpAGQAYQBkACAA
ZABlACAAQuBlIAHIAdADpAGYAaQBjAGEAYwBpAPMAbgAgAEkAbgB0AGUAcgBtAGUAZABpAGEAIABk
AGUAIABsAGEAIABBAEMAQuBWACAAKABBAGcAZQBuAGMAaQBhACAAZABlACAAVABlAGMAbgBvAGwA
bwBnAO0AYQAgAHkAIABDAGUAcgB0AGkAZgBpAGMAYQBjAGkA8wBuACAARQBsAGUAYwB0AHIA8wBu
AGkAYwBhACwAIABDAEkARgAgAFEANAA2ADAAMQAxADUANgBFACkALgAgAEMAUABTACAAZQBuACAA
aAB0AHQAcAA6ACSALwB3AHcAdwAuAGEAYwBjAHYAIgBlAHMwMAYIKwYBBQUHAgEWJGh0dHA6Ly93
d3cuYWNjdS5cy9sZWQdps2ubY2lnbHjLmhlbTBVBgNVHR8E TjBMMEigSKBGhkRodHRwOi8vd3d3
LmFiY3YuZXMvZmlsZWFkbWluL0FyY2hpdm9zL2NlcnRpZmlyYWRvcy9yYWI6YWNjdjFZGVyLmNy
bDAOBgNVHQ8BAf8EBAMCAQYwFwYDVR0RBBawDoEMYWNjdkBhY2N2LmVzMA0GCSqGSlb3DQEBBQUA
A4ICAQA+fFVGYa3zf/b1GQ1MTdYUHsSbAIA5esf2htyAzeca/OHu2CRgGXajCbJN7cC2pFuhsiWY
Xrnhjuc/crzzrYYYjzRsO8iQn7+/hgs56wzRCQvxMy0lLrwiVPXxtdgs8mU1MMGq13T+Nthkq3uotX
XZgxUu3Zhvt9kK2wDVwxtLIp/McQpRcl1VSCSgvGg/IteIi7+NQ2wBQPbyGamigxFI7LDkgio0
sI2K6qV4q43pYpGq3YidDE/ssEBLSkT2IlHLgqZL9An5gVoer6vCK58XJx9FGCpVtksUQYnm+cAk
NxzV/cAfWIZroQwiF+vUSy8bjuPRslpszoWFAJ7wg50OHaigU/kfT7KMA/2RtpmxaGKB0thURRrcz
dGB/k1IpKjG8N3zjw2StkWqdGXFnlxdfxv9wr1/ultrA7QPT62kWDPY959ZVCOoGxuIz9ExH2NS2tw
bzHRbQqI8/VpeSkepE2ffjMkqo6oU/7IlxyLCDZ3CqvlbXXxGlW4hvWiV76tN6b7fEo8NxSkz0FzyA
tD/H2pdd/RkTL0LSLj7FalowiP6svMeFgxJoecmEt6TrUGffFgQggyLiPdEalB0zSbs2m0ErwIbk
KkQY1bh+vAoK0bHa35KOFYySijGXbu93Imz+LaKsARIBqQ/ZPP2eOZ2FWP+k5wcZYyxNpeI.0dtz7
svdTIw==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer C: *ES*

Issuer O: *ACCV*

Issuer OU: *PKIACCV*

Issuer CN: *ACCVRAIZ1*

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-120*

Valid from: *Thu Oct 13 16:55:04 CEST 2011*

Valid to: *Fri Jan 01 00:59:00 CET 2027*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9B:06:23:17:1E:D2:66:66:AB:2E:3D:3E:EC:3A:9D:26:7E:AA:B7:91:30:3E:98:17:C6:71:33:CC:57:CE:49:0A:D2:9B:
AC:A5:82:50:01:8D:54:C4:CE:79:7D:6B:99:BF:C9:D3:40:C6:08:15:18:A3:40:FA:13:AC:14:26:A0:15:2E:4F:EA:72:7C:6D:9E:12:65:B2:0B:A5:9E:9E:81:4A:17:0D:5F:FE:23:2D:05:81:6E:EC:24:B3:CF:87:7D:B7:D8:EB:5E:
BF:14:A2:C0:61:3C:8A:98:C9:05:56:55:3F:EA:98:30:51:29:79:D9:0B:44:8D:87:CC:5D:17:56:B9:92:F5:87:D6:3B:32:BB:CA:1D:BE:77:80:AA:3C:27:D7:D5:6D:1A:19:E0:4A:DB:5B:24:00:15:C4:5D:E4:60:64:3A:F5:53:99:
26:2D:16:40:A0:6E:4D:64:1E:97:3D:C5:5D:B9:D0:6F:95:ED:F3:3B:69:C5:3E:56:1E:0C:CB:11:48:E0:45:C1:0A:74:2F:BB:5C:11:9D:5D:43:6B:BF:BA:1A:B7:51:F2:46:7A:C5:AD:B2:19:FF:FF:FB:10:0C:2F:0A:ED:35:FD:C
2:19:51:93:0E:90:C7:95:7C:4D:C3:B9:C5:03:49:6B:10:50:9E:C3:41:C3:8D:53:05:7E:2C:82:5C:33:17:9D:30:7C:0D:97:9F:43:D2:E0:68:53:D2:6B:3F:8A:37:AA:22:1D:59:3F:B7:81:29:CE:29:B0:C3:49:66:DC:E1:8D:D5:02:7
8:AE:96:6D:94:43:A8:AE:FC:1A:FF:4A:F7:DE:68:C4:51:03:99:1F:4A:C9:BE:63:0C:78:06:57:CA:91:76:2B:A9:E6:0D:22:6A:73:12:83:68:94:E5:1C:46:CE:3B:DD:19:42:C3:80:09:AF:27:F7:C1:B8:23:2F:D7:9A:CB:B3:3F:1
C:E3:36:31:34:36:CD:1D:17:C4:4F:A4:E5:C4:46:6D:2C:AD:70:18:BD:E5:AD:78:17:00:D5:CB:15:64:90:CD:3C:39:12:00:70:B9:E0:96:31:90:C8:96:F8:B8:C7:5E:A8:79:7E:46:ED:07:2B:2A:B4:12:F0:30:9D:5A:11:A5:84:33
:15:24:E7:01:92:42:C9:B6:54:63:2A:2B:66:62:24:C8:A1:18:85:69:1B:78:4B:8F:8B:FB:4D:38:AC:79:5C:6E:BF:44:73:BE:87:6D:29:81:62:C9:AE:21:FA:E4:F2:74:8F:0C:69:EF:D0:B3:A8:AC:C8:5A:5D:D7:27:E9:CE:51:66:9
1:F4:D3:C9:6F:E9:F3:79:C2:92:DE:12:44:2E:CC:68:C0:4C:B4:C5:6E:8F:02:03:01:00:01

Authority Info Access *http://ocsp.accv.es*

Subject Key Identifier *E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5*

Basic Constraints *IsCA: true*

Authority Key Identifier *D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]

CPS pointer: http://www.accv.es/legislacion_c.htm

CRL Distribution Points

http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

Subject Alternative Name

accv@accv.es

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

3B:C5:18:56:04:0A:D7:FF:66:83:AA:85:A0:D3:4F:9E:A6:80:CD:23:C3:7C:B8:A0:42:3B:0F:89:A2:44:05:B9

Certificate fields details

Version:

3

Serial Number:

4753158885672534199

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHkjCCBXqgAwIBAgIIQfac0r2AwLcwDQYJKoZIhvcNAQELBQAwQjESMBAGA1UEAwwJQUNDVlJB
SVoxMRAwDgYDVQQLDAdQS0lBQ0NWMQ0wCwYDVQQKDARBQ0NWMQswCQYDVQQGEwJFUzAeFw0xNTAx
MjcxNDA2NDJaFw0yNjEyMzEyMzU5MDBaMEMxEzARBgNVBAMMCkFDQ1ZDQS0xMjAxIDA0BgNVBAsM
B1BLSUFDQ1YxDTALBgNVBAoMBEFDQ1YxCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAmwYjFx7SZmarI_j0+7DqdJn6qt5EwPpgXxnEzzFfOSQrSm6ylglABjVTEznl9
a5m/ydNAxggVGKNA+hNMFCagFS5P6nJ8bZ4SZbILpZ6cgUoXDV/+Iy0FgW7sJLPPh3232OtevxSi
wGE8tpJBVZVP+qYMFEpedkL Rl2Hzf0XVrmS9YlWOzK7yh2+z4dCqPCTX1W0uGcBK21skAtBXEXcRg
ZDr1U5kmLRZAoG5NZB6XPcVdudBvIe3zO2nFPlYeDMsRSOBFwQp0L7tcEZ1dQ2u/uhq3UlJGesWt
shn//sQDC8K7TX9whlRkw6Qx5V8TcO5xQNJaxBQnsNBw41TBX4sglwzF50wfA2Xn0PS4GhT0ms/
ijeqIh1ZP7eBKc4psMNJZtzhjdUCcK+WbZRDqK78Gv9K995oxFEDmR9Kyb5jDHgGV8qRdiup5g0i
anMSg2lU5RxGizyvdGUUDgAmvJfBuCMv15rLsz8c4zYxNDbNHRET6TlxE2LK1wGL3lrXgXANXL
FWSQzTw5EgBwueCWMZDlIvi4x16oeX5G7QcrKrQS8DCdWhGlhDMVJOcBkkLJtlRjKitmYiTloRiF
aRt4S4+L+004rHlcbr9Ec76HbSmBYsmulfik8nSPDGnv0LOorMhaXdcn6c5RZpH008Iv6fN5wpLe
EkQuzGjA1LTFbo8CAwEAAaOCAokwggKFMC8GCCsGAQUFBwEBBCMwITAfBggrBgEFBQcwAYYTaHR0
cDovL29jc3AuYWNjdi5kczAdBgNVHQEFgQU6ECbytmP8FE2KH1EgBQggXy+UwIwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMEGDAWgBTSb7Tj3zcnk1X2VuqB5TbMjB4/vTCCAX8GA1UdIASCAXYwggFy
MIIBbgYEVR0gADCCAWQwggFuBggrBgEFBQcCAjCCASAeggEcAEEAdQB0AG8AcgBpAGQAYQBkACAA
ZABlACAAQwBlAHIAdABpAGYAaQBjAGEAYwBpAPMAbgAgAEkAbgB0AGUAcgBtAGUAZABpAGEAIABk
AGUAIABsAGEAIABBAEMAQwBWACAAKABBAGcAZQBuAGMAaQ8bACAAZABlACAAVABlAGMAbgBvAGwA
bwBnAO0AYQAgAHkAIABDAGUAcgB0AGkAZgEBpAGMAYQBjAGkAwBuACARQBkAGIAYwB0AHIAbwBu
AGkAYwBhACwAIABDAEkARgAgAFEANAA2ADAAMQAxADUANgBFACkALgAgAEMAUABTACAAZQBuACAA
aAB0AHQAcAA6AC8ALwB3AHcAdwAuAGEAYwBjAHYALgBlAHMwMAYIKwYBBQUHAgEWJGh0dHA6Ly93
d3cuYWNjdi5lcy9sZWdpc2xhY2lvb9jLmh0bTBVBgNVHR8ETjBMMEggSKBGhkRodHRwOi8vd3d3
LmFjY3VaZXMvZmlsZWFkbWlul.0FyY2hpdnr9zL2NlcnRpZmlj YWRvcy9yYWl6YWNjdjFZGVyLmNy
bDAOBgNVHQ8BAf8EBAMCAQYwFwYDVR0RBBAwDoEMYWNjdkBhY2N2LmVzMA0GCSqGSIb3DQEBCwUA
A4ICAQAcslCqv3AJB2/QNQLL2mkFaf0Q/X9uU/idWzhEQYHOF+Eh9ojMea/o+6rzgmrXEHOPIyoE
OX7vKzAsQca/w7cM/ldWB4Q3yN6Bv07OyA7EKkTLpL8X0VSJV2XgxDRpAsvJ+hqPPPIo4DW7AAk
8zfZ+j92OG2WkHEWzEHXA68MstCxxpcwAYHdRuCsH6CD+dRmODCzCRc9NsanhLOX3JPzRbc4i
tMAR1YK4uHCqj/VwFLd+oT84cAksXpNd2qBslCXgfVV0B1w+Efj7aaDCw9gY0lbtPMvpadiwjq1m
YATBW8+jLb3i2YfRx5fi0YXcv68Hjvb5zDexgMdbkqxHjPvmsfkFmzYDRzxZkYhqcMHLxzZlKD7F
1Sa2GYM/kuG7n7zHGuodg3sWzLN16jbaHbupjTT6L4sVqQVW56wct9zaDD38rl0Nn/u5ch5K
oih1OB2FOmH2kA0YMRpPkvDy2SQZLVG95M8GBBVQu97Bd7/7b3RQr4nYSMLNXzbZPhjuLLMg5q
OZNuLhrS09nWcyeAYp6pA4KmNgJtLnRBw6+j5b6+RMQpdoxY8AQm301OjK3KsVB+IktHpcv7aDcw
WWup9ZF7SAbgmy0dig0n8+AofQQnYbi0jgcdjguxsvYznwgf+SsIIF+BTEMSGWi5MDbppe3b+Tbq
sRDXGA==

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer C:

ES

Issuer O:

ACCV

Issuer OU:

PKIACCV

Issuer CN:

ACCVRAIZ1

Subject C:

ES

Subject O:

ACCV

Subject OU:

PKIACCV

Subject CN:

ACCVCA-120

Valid from:

Tue Jan 27 15:06:42 CET 2015

Valid to:

Fri Jan 01 00:59:00 CET 2027

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9B:06:23:17:1E:D2:66:66:AB:2E:3D:3E:EC:3A:9D:26:7E:AA:B7:91:30:3E:98:17:C6:71:33:CC:57:CE:49:0A:D2:9B:AC:A5:82:50:01:8D:54:C4:CE:79:7D:6B:99:BF:C9:D3:40:C6:08:15:18:A3:40:FA:13:4C:14:26:A0:15:2E:4F:EA:72:7C:6D:9E:12:65:B2:0B:A5:9E:9E:81:4A:17:0D:5F:FE:23:2D:05:81:6E:EC:24:B3:CF:87:7D:B7:D8:EB:5E:BF:14:A2:C0:61:3C:8A:98:C9:05:56:55:3F:EA:98:30:51:29:79:D9:0B:44:8D:87:CC:5D:17:56:B9:92:F5:87:D6:3B:32:BB:CA:1D:BE:77:80:AA:3C:27:D7:D5:6D:1A:19:E0:4A:DB:5B:24:00:15:C4:5D:E4:60:64:3A:F5:53:99:26:2D:16:40:A0:6E:4D:64:1E:97:3D:C5:5D:B9:D0:6F:95:ED:F3:3B:69:C5:3E:56:1E:0C:CB:11:48:E0:45:C1:0A:74:2F:BB:5C:11:9D:5D:43:6B:BF:BA:1A:B7:51:F2:46:7A:C5:AD:B2:19:FF:FF:FB:10:0C:2F:0A:ED:35:FD:C2:19:51:93:0E:90:C7:95:7C:4D:C3:B9:C5:03:49:6B:10:50:9E:C3:41:C3:8D:53:05:7E:2C:82:5C:33:17:9D:30:7C:0D:97:9F:43:D2:E0:68:53:D2:6B:3F:8A:37:AA:22:1D:59:3F:B7:81:29:CE:29:B0:C3:49:66:DC:E1:8D:D5:02:78:AF:96:6D:94:43:A8:AE:FC:1A:FF:4A:F7:DE:68:C4:51:03:99:1F:4A:C9:BE:63:0C:78:06:57:CA:91:76:2B:A9:E6:0D:22:6A:73:12:83:68:94:E5:1C:46:CE:3B:DD:19:42:C3:80:09:AF:27:F7:C1:B8:23:2F:D7:9A:CB:B3:3F:1C:E3:36:31:34:36:CD:1D:17:C4:4F:A4:E5:C4:46:6D:2C:AD:70:18:BD:E5:AD:78:17:00:D5:CB:15:64:90:CD:3C:39:12:00:70:B9:E0:96:31:90:C8:96:F8:B8:C7:5E:A8:79:7E:46:ED:07:2B:2A:B4:12:F0:30:9D:5A:11:A5:84:33:15:24:E7:01:92:42:C9:B6:54:63:2A:2B:66:62:24:C8:A1:18:85:69:1B:78:4B:8F:8B:FB:4D:38:AC:79:5C:6E:BF:44:73:BE:87:6D:29:81:62:C9:AE:21:FA:E4:F2:74:8F:0C:69:EF:D0:B3:A8:AC:C8:5A:5D:D7:27:E9:CE:51:66:91:F4:D3:C9:6F:E9:F3:79:C2:92:DE:12:44:2E:CC:68:C0:4C:B4:C5:6E:8F:02:03:01:00:01

Authority Info Access

http://ocsp.accv.es

Subject Key Identifier

E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5

Basic Constraints

IsCA: true

Authority Key Identifier

D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]

CPS pointer: http://www.accv.es/legislacion_c.htm

CRL Distribution Points

http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

Subject Alternative Name

accv@accv.es

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

2D:E6:20:F2:D1:20:0A:A9:0B:16:C3:CC:F6:70:FD:7E:D1:43:79:AB:06:FA:8B:03:1C:FE:F8:DA:05:1E:A5:A2

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-120*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2018-01-16T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

10.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.16.3.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.17.3.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.14.3.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.15.3.0*

10.5.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.7.5.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.6.6.0*

10.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

10.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

10.5.6 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ACCVCA-120*
Name	*[es]*	*Certificados Reconocidos emitidos por ACCVCA-120*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject O:	*ACCV*
Subject OU:	*PKIACCV*
Subject CN:	*ACCVCA-120*

X509SKI

X509 SK I	*6ECbjvtmP8FE2KHf1EqBQggXy+U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

10.5.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.16.3.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.17.3.0*

10.5.6.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.7.5.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.6.6.0*

10.5.6.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.5.7 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ACCVCA-120*
Name	*[es]*	*Certificados Reconocidos emitidos por ACCVCA-120*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject O:	*ACCV*
Subject OU:	*PKIACCV*
Subject CN:	*ACCVCA-120*

X509SKI

X509 SK I	*6ECbjvtmP8FE2KHf1EqBQggXy+U=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2012-04-15T22:00:00Z*

10.5.7.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.16.3.0*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.8149.3.17.3.0*

10.5.7.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
	[es]	*está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.7.5.0*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.8149.3.6.6.0*

10.6 - Service (granted): Qualified Certificate issued by ACCVCA-130

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificate issued by ACCVCA-130*

Name *[es]* *ACCVCA-130*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6022689390316330646*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHkjCCBXqgAwIBAgIIU5TkF0ZRnpYwDQYJKoZIhvcNAQELBQAwQjESMBAGA1UEAwwJQUNDVUJB
SVoxMRAwDgYDVQQLDAdQS0lBQ0NWMQ0wCwYDVQQKDARBQ0NWMQswCQYDVQQGEwJFUzAeFw0xNTAx
MTUxMDIzMjRaFw0yNjEyMzEyMzU5MDBaMEMxEzARBgNVBAMMCkFDQ1ZDQS0xMzAxEDAOBgNVBAsM
B1BLSUFDQ1YxDTALBgNVBAoMBEFDQ1YxCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAo5KJruh7JPEBxpdC8Pf3qN8vtPR98dCWZynbjLBXv6MTjwAiehTq1X8OzEQN
pqWgpNpygo6/YNgt8FMgYWhCsPSDvEmg5Um1xBnLjHBJMSlP7VCIMVS9KidVu+nF8PpZno8hecsf
F4yJzLpMD/ha8sjdt5Zp9ee8cVBJkSkRJDY4gWITWRYO0kr1ZQSmu+2+YKyZZRp0Po6k4eGIlsFG
z9ylzVi0hasDf43Lv19F515tNGXFIYmNnLjMFl/LKuAI87jblGqRn5yhMGuJNsP05gH5D/F5Yk
Lgg6A83KmygsIsgYzN72YWiFYNzB6ZzF0HPM9GX3PuSkKKXyFpUxYL0nHWH7B3Sc4F5m+mmFk9GM
vJVuoUvktOO2ysFPE3pYtI1JjrVGBk5cmZHKQbqBw5ZooSEJNbmvtzshUxVEFTDRg+8avleaZFN
vl5hiISQ4c7YlwSnu80AMfhUpD6bwA+7BG91clQdcoMuedHyvE3IGqYxuh25a3u/K97joz+qq1
0hzHSeNrExjWV20DIf6kgZqo6C2p0zm5eTIbaZ16oVZrpmTcG95dabQzgHDdXP6B4el67G275jQ
Nok2Wu5wT9oKAM6xomNp6zsr0uYI9kQBqMP8BTPliB98rwg9xmQH4Ss/r1zZK3xt+mYypBo1ORSV
vKEEqs1bnVI3LjMCAwEAAaOCAokwggKFMC8GCCsGAQUFBwEBBCMwITAfBggrBgEFBQcwAYYTaHR0
cDovL29jc3AuYWNjdi5lcyAdBgNVHQ4EFgQUSS9DFi3YMFTV4Yt+1YDi/6fxblwDwYDVR0TAQH/
BAUwAwEB/zAfBgNVH5MEGDAWgBTSb7Tj3zcnk1X2VuqB5ThMjB4/vTCCAX8GA1UdIASCAXYwggFy
MIIBbgYEVR0gADCCAWQwggEuBggrBgEFBQcCAjCCASAeggEcAEEAdQB0AG8AcgBpAGQAYQBkACAA
ZABlACAAQwBlAHIAdABpAGYAaQBjAGEAYwBpAPMAbgAgAEkAbgB0AGUAcgBtAGUAZABpAGEAIABk
AGUAIABsAGEAIABBAEMAQwBWACAAKABBAGcAZQBuAGMAaQBhACAAZABlACAAVABlAGMAbgBvAGwA
bwBnAO0AYQAgAHkAIABDAGUAcgB0AGkAZgBpAGMAYQBjAGkAbwBuACAARQBsAGUAYwB0AHIAbwBu
AGkAYwBhACwAIABDAEkARgAgAFEANAA2ADAAMQAxADUANgBFACkALgAgAEMAUABTACAAZQBuACAA
aAB0AHQAcAA6AC8ALwB3AHcAdwAuAGEAYwBjAHYALgBlAHMwMAYIKwYBBQUHAgEWJGh0dHA6Ly93
d3cuYWNjdi5lcy9sZWdpc2xhY2lvbi9lLmh0bTBVBgNVHR8ETjBMMEggSKBGhkRodHRwOi8vd3d3
LmFjY3YuZXMvZmlsZWFkbWluL0fyY2hpdm9rL2NlcnRpZmlyYWRvcy9yYWl6YWNjdjFZZGVyLmNy
bDAOBgNVHQ8BAf8EBAMCAQYwFwYDVR0RBBAwDoEMYWNjdkBh6Y2N2LmVzMA0GCSqGSIb3DQEBCwUA
A4ICAQAs1zQb+upsV3E5Xb2heesc2RLziFGzxBqyRiGgzl7aZBtg4fAwbl6TvjwEtZHbGkW+DxYz
J4EvgI+U8Cbbwm9GVGUNA5e0l1byywJYgd/y2v8gGX+zM7X8mowih1zPIN6Z5ode2abCNXylIfhL
WeGKnOLjzzY1+Jxtv6bWu7Z29ZrU2++SSbOwjvSLtaIz1zN+OkqzKv1TBk4O8xcgBXcgRf8XZfWs
oHX+wQpZhUZuIZxYvm4FLXbb+1eHE2rNwkbrBbBM0MNGxP8DFIH8IfEkVDrJgk2sW8drvcbU01D9
IwIcP9YVY4Rsq4Qesu8psHyr1HyLr+IoyqsdKLjUQ4o67o7ITWHhl04mW9wz0kREn/siqR+chY2z
RpIO7hGwl64TIBYuIWxdOavqDKMeHJjLKJVOsYsWK4X9fjnP+5+wFSAM+0zINDbezBAIM1p0sd5DV
9KrQZ9TE9PxT1G0dvWnJRbp6PRVruvvr+vSzGBLjWY5r8PaKsseAKtjFUi52s2BH3L10+UMO+q
LWVohAyOygNYkv5eVSW3XLn3NzgVh5QZrHs7IalcpHLPnyMW1YkN0l+cqCXVgTNVFGkJup4TJcl
2gw1sYi4z7FadKTi9c91ZSuYN4Zb+qtM8ysaB1bg7UfU+dAry8nFxuHeo4MhiF6cx7HxobOy2p7r
iigccw==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer O: *ACCV*

Issuer OU: *PKIACCV*

Issuer CN: *ACCVRAIZ1*

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-130*

Valid from: *Thu Jan 15 11:23:24 CET 2015*

Valid to: *Fri Jan 01 00:59:00 CET 2027*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A3:92:89:AE:E8:7B:24:F1:01:C6:97:42:F0:F7:F7:A8:DF:2F:7C:F4:7D:F1:D0:96:67:29:DB:8C:B0:57:BF:A3:13:8F:0 0:22:7A:14:EA:D5:7F:0E:CC:44:0D:A6:A5:AA:A4:DA:72:82:8E:BF:60:D8:1F:F0:53:20:61:68:42:B0:F4:83:BC:49:A0:E5:49:B5:C4:19:CB:8C:70:49:31:22:0F:ED:50:A5:31:54:BD:2A:27:55:BB:E9:C5:F0:FA:59:9E:8F:21:7 9:CB:1F:17:8C:89:CC:BA:7F:30:3F:E5:C0:8B:23:92:1E:59:A7:D7:BA:71:50:49:B1:29:11:24:36:38:81:69:53:59:16:0E:FF:47:B5:65:04:A6:BB:ED:BE:60:AC:B6:65:1A:4E:3E:8E:A4:E1:E1:A5:22:C1:46:CF:DC:88:CD:58:A 2:D2:16:AC:0D:FE:37:2E:FD:7D:17:9D:79:B4:D1:97:14:86:26:36:72:E3:30:59:5F:FC:B2:AE:02:5F:3B:8D:B9:46:A9:19:F9:CA:13:06:B8:93:6C:3F:4E:60:1F:90:FF:17:96:24:2E:A8:3A:03:CD:CA:9B:28:2C:22:C8:18:CC:DE :F6:61:68:85:60:DC:C1:E9:9C:C5:D0:73:CC:F4:65:F7:3E:E4:A4:28:A5:F2:16:95:31:60:BD:27:1D:61:FB:07:74:9E:E0:5E:66:FA:69:85:93:D1:8C:BC:95:6E:A1:4B:E4:B4:E3:B6:CA:C1:4F:13:7A:58:B6:5D:62:26:3A:D5:18:1 9:39:72:66:47:29:06:EA:07:0E:59:A2:84:84:24:D6:E6:BE:DC:EC:85:4C:55:10:54:C3:46:0F:BC:6A:F9:5E:69:91:4D:BE:5E:61:8A:54:90:E1:CE:D8:96:F4:A7:BB:CD:00:31:F8:49:FE:90:FA:6F:00:3E:EC:11:BD:D5:E9:50:75: CA:0C:B9:E7:47:CA:F1:37:94:6A:98:C6:E8:76:E5:AD:EE:FF:F2:BD:EE:3A:33:FA:AA:B5:D2:16:47:E5:E3:6B:13:18:D6:57:6D:03:94:5E:A4:81:9A:A8:E8:2F:F6:A7:4C:E6:E5:E4:DF:6D:A6:75:EA:85:59:AE:99:93:78:6F:7 9:75:A6:D0:CE:01:C3:75:73:FA:07:87:A5:EB:B1:B6:EF:98:D0:36:89:36:5A:EE:70:4F:DA:0A:00:CE:B1:A2:63:69:EB:3B:2B:D2:E6:08:F6:44:01:A8:C3:FC:05:33:E5:88:1F:7C:AF:08:3D:C6:64:07:E1:2B:3F:AF:5C:D9:2B:7 C:6D:FA:66:32:A4:1A:35:39:1E:55:BC:A1:04:AA:CD:5B:9D:57:F7:2E:33:02:03:01:00:01

Authority Info Access *http://ocsp.accv.es*

Subject Key Identifier *E5:27:FD:0C:58:B7:60:C1:53:57:86:2D:FB:56:03:8B:FE:9F:C5:B2*

Basic Constraints *IsCA: true*

Authority Key Identifier *D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]

CPS pointer: http://www.accv.es/legislacion_c.htm

CRL Distribution Points *http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl*

Subject Alternative Name *accv@accv.es*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *57:2B:F8:99:FD:77:43:62:DC:19:21:96:25:EC:C1:57:BB:55:43:4E:A5:16:6D:57:58:DC:4B:4F:89:0 D:66:53*

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-130*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

10.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.6.2 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificate issued by ACCVCA-130*

Name *[es]* *ACCVCA-130*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-130*

X509SKI

X509 SK I *5Sf9DFi3YMFTV4Yt+1YDi/6fxbI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-23T22:00:00Z*

10.7 - Service (granted): Qualified timestamps issued by 'TSA1 ACCV 2016'

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by 'TSA1 ACCV 2016'*

Name *[es]* *Sellos cualificados de tiempo emitidos por 'TSA1 ACCV 2016'*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *969592673683204365*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIYDCCBkigAwIBAgIIDXSvZku1aQ0wDQYJKoZIhvcNAQELBQAwQjESMBAGA1UEAwwJQUNDVlJB
SVoxMRAwDgYDVQQLDAdQS0lBQ0NWMQ0wCwYDVQQKDARBQ0NWMQswCQYDVQQGEwJFUzAeFw0xNjAy
MjkxNjM3NTBaFw0yOTAyMjUxNjM3NTBaMIGkMRcwFQYDVQQDDA5UUl0ExIEFDQ1YgMjAxNjEQMA4G
A1UECwwHUlEiJQUNDVjFEMEIGA1UECgw7QWdlbmNpYSBkZSBUZWNub2xvZ8OYSBlIENlcnRpZmIj
YWNpw7NuIEVsZWN0csOzbmljYSAtIEFDQ1YxETAPBgNVBAcMCFZhbGVuY2lhMREwDwYDVQQIDAbW
YWxlbmNpYTELMAkGA1UEBhMCRVMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC5E8Sz
uMnjbK3DwMMCEQmnW839Mm0yQEMphI0qCw91YXRO4668c/AX4PnLMZEoTGAgMoAUZfdexXgRnQOx
HJt94Ujzs88I1A/6Qm0jWLNDHXS6iIL1FDIqWxDEPWb3vb2Qeeu3CjxLW0pgw5VtIbmuXbg8pk4QVYm
S96I1ZXVcY7mgXIluK0QE0ovEjyVOOYGaV6sxfX2bGhzkGpL/4b5na4cDde9vHW9qrQYbKBpRygGUr
MiH1odj60XO6bD1thZx/CAcWIVjp1jkqireglWzu5X2TvUHw0xIMTpCGMQ1KgKzvxLMw6sD2MA+4m
TQTWzEaFaTT5I4aGwFqT4Q4O4Ap5xbc612DwA8w11FZfIIENNT1q5LYGqQ27DP3+AfrdZWXiCLRM
cmOYZ6qSChOcM3aFARiGJadTp1F/S483xIj+HpCq0Uso1aQXCdUVK/YWY5av+4uiC7x3WFIdAJCo
fAu0Ilg7Fmn/mypBGrqnDgzEIZSp3M/+zqqJxPrIbs0LOVQQLszO0QtBwPSHsR+UNTD55Vcc4wg
TGsT6mutve+8zcfRkgeyK0pC3XIWCHxOqGI2aYrgGyuXMJH0axa1UgIJmKbmiy0SmCcxOhMr16GO
hL2b96jRkXKPoPb1GY/EoB9sik3H85L0vCnGKSTswPd6pu1Ng/auKQDW0q12Sq1EOoK9CQIDAQAB
o4IC9TCCAvEwZgYIKwYBBQUHAQEEWjBYMDUGCCsGAQUFBzAChilodHRwOi8vd3d3LmFjY3YuZXMv
Z2VzaGNlcnQvQUNDVUBSVoxLmNvdDAtBggrBgEFBQcwAYYTaHR0cDovL29jc3AuYWNjdi5lczAd
BgNVHQ4EFgQUxsTYQMbIl2dS1HD+k7VDlRiIZQwHwYDVR0jBBgwFoAU0oe04983J5NV9lbqgeU2
zfweP70wggHGBgNVHSAEggG9MIIBuTCCAbUGCysGAQQBv1UDZAIAMIIBpDCCAW4GCCsGAQUFBwIC
MIIBYB6CAVwAUwBlAHIAdgBpAGQAbwByACAAZABlACAAUwBlAGwAbABhAGQAbwAgAGQAZQAgAFQA
aQBlAG0AcABvACAAZABlACAAbABhACAAQQBnAGUAbgBjAGkAYQAgAGQAZQAgAFQAZQBjAG4AbwBz
AG8AZwDtAGEAIAB5ACAAQwBlAHIAdABpAGYAaQBjAGEAYwBpAPMAbgAgAEUAbABlAGMAdAByAPMA
bgBpAGMAYQAgAEkAVgBGACAAKABQAGwALgAgAGQAZQAgAE4AYQBwAGSAbABlAHMAIAB5ACAAUwBp
AGMAaQBsAGkAYQAgADYALAAgAEMAUAAgADQANgAwADAAMwAgAEMASQBGACAAUQA5ADYANQAwADAA
MQAwAEMAKQAuACAAQwBQAFMAIAB5ACAAQwBQACAAZQBuACAAaAB0AHQAc4AC8ALwB3AHcAdwAu
AGEAYwBjAHYALgBlAHMwMAYIKwYBBQUHAgEWJGh0dHA6Ly93d3cuYWNjdi5lcy9sZWdpc2xbY2lv
bl9jLmh0bTBVBgNVHR8ETjBMMEggSKBGhkRodHRwOi8vd3d3LmFjY3YuZXMvZmlsZWFkbWluI0Fy
Y2hpdm9zL2NlcnRpZmljYWRvcy9yYWl6YWNjdjFlZGVyLmNybDAOBgNVHQ8BAf8EBAMCBsAwFgYD
VR0lAQH/BAwwCgYIKwYBBQUHAwgwDQYJKoZIhvcNAQELBQADggIBAAjWDDA6ddmDPJ1t09dU//0/7
VbuCwqOhMONk8Phr+Nfot/AxWsDk8OYa1CuGNGHvyKxs0ygL3MNJFxnr+UE0PnYhZ7wz8zzTsI
9p5G3bB/7Euvw1s55/+4kxypGoJeJYY8+Jax9pT+x1VuZF5Uvv2ic7gQCYwa5X0gSGXAdVgzKLYL
uvzovitpkuIgbDmVmhGw36GvLQ6FAtxQJb2Mmgfubo7RBlirxgMlKyBwxZReb7VWN6dTACm9335j
CY/pSgio11iGpNRcRITKRIU58yosdZa239gZU+3TxsfNtfwuIMSTg58lYvHEutHKKgtlhACdKm8J
waX1Flu6gmI6ZwzBKUgXb9sxUFdHIIza0IeYzUg11DD6/CkqtuygnVNQlbAaKfNBsMwbQS0nOS
bMq1azIZNuoF6Oo9cIHSCz7jEKt+1xMYk/Lmq4ZUdE0IuQ2tezadOXn/B6rqDc4xFhKKcTUt2Vpr
TUKGWCXTX49FwhDdmyP3/BlL62NkvIALorjD2GiW4WqaOicefE2yVmqv4H9gh4F70eEa8CPqxYY7
5MImIoQGtzk49vcDe63Yji1ZsTY7Ju4k8z9YKeDjio7DZ1c1NoQOeadIoEbACBeb2NScosghLACz
+Pj0O2eOo1Liu2e49OnEcSVSzVZz82q2Bm7BmUjTpgZyvVhlhgIA

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer O: *ACCV*

Issuer OU: *PKIACCV*

Issuer CN: *ACCVRAIZ1*

Subject C: *ES*

Subject ST: *Valencia*

Subject L: *Valencia*

Subject O: *Agencia de Tecnología y Certificación Electrónica - ACCV*

Subject OU: *PKIACCV*

Subject CN: *TSA1 ACCV 2016*

Valid from: *Mon Feb 29 17:37:50 CET 2016*

Valid to: *Sun Feb 25 17:37:50 CET 2029*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B9:13:C4:B3:B8:C9:E3:6C:AD:C3:C0:C3:02:11:09:A7:5B:CD:FD:32:6D:32:40:43:29:85:FD:2A:0B:0F:75:61:74:4E:E3:AE:BC:7B:F0:17:E0:F9:CB:31:91:28:4C:60:20:32:80:14:65:F7:5E:C5:78:11:9D:03:B1:1C:9B:7D:E1:48:F3:F3:C2:75:03:FE:90:98:E8:D6:2C:D0:C7:5D:2E:87:2C:50:C8:A9:6C:43:10:F5:9B:DE:F6:F6:41:E7:AE:DC:28:F1:2D:6D:29:83:0E:55:B4:37:A7:B9:76:E0:F2:99:38:41:56:26:4B:DE:87:D5:95:D5:FD:E6:26:81:71:EE:2B:44:04:D2:8F:C4:8F:25:4E:39:8E:9A:57:AB:31:7D:7D:A1:1A:1C:E4:1A:95:38:6F:99:DA:E1:C0:F8:7B:DB:C7:5B:DB:29:41:86:CA:06:94:72:80:65:2B:32:21:F5:A1:D8:FA:D1:73:9B:0F:57:E1:67:1F:C2:01:C5:9F:56:9D:63:92:A8:AB:7A:08:96:CE:EE:57:D9:3B:D4:1F:0D:31:20:C4:E9:08:63:10:D4:A8:0A:CE:FC:4B:33:0E:AC:0F:63:00:FB:8A:E7:4D:04:D6:CC:46:85:69:34:F9:97:86:86:C0:5A:93:E1:0E:0E:E0:0A:79:C5:B7:3A:D7:60:F0:03:CC:08:D4:56:5F:7C:91:0D:35:39:6A:E4:B6:06:A9:0D:BB:0C:FD:FE:01:FA:DD:65:65:E2:08:B4:4C:7A:63:98:67:AA:92:0A:13:9C:33:76:85:01:18:86:25:A7:53:A7:51:7F:4B:8F:37:C4:88:FE:1E:90:AA:D1:4B:28:1D:A4:17:09:D5:15:2B:F6:16:63:96:AF:FB:8B:A2:0B:BC:77:58:52:1D:00:90:A8:7C:0B:B4:12:0E:C5:B6:6F:E6:CA:CA:41:1A:BA:A9:0E:0C:C4:25:9E:69:DC:CF:FE:CE:3A:89:C4:FF:DF:95:2D:0B:39:54:10:2E:C8:D9:D3:84:2D:07:03:D2:1E:C4:7E:50:D4:C3:E7:95:5E:73:8B:EA:4C:6B:13:EA:6B:AD:BD:EF:BC:CD:C7:D1:92:07:B2:2B:4A:42:DD:77:D6:08:7C:4E:A8:62:36:69:8A:E0:1B:2B:97:30:91:F4:6B:16:B5:52:0D:49:98:A6:E6:8B:2D:12:98:27:31:3A:13:2B:D7:A1:8E:84:BD:9B:F7:A8:D1:91:72:8F:A0:F6:F5:19:8F:C4:A0:1F:6C:8A:4D:C7:F3:92:F4:BC:29:C6:29:24:EC:C0:F7:7A:A6:ED:4D:83:F6:AE:29:00:D6:D2:AD:76:4A:AD:44:42:82:BD:09:02:03:01:00:01

Authority Info Access

http://www.accv.es/gestcert/ACCVRAIZ1.crt

http://ocsp.accv.es

Subject Key Identifier *C6:C4:D8:40:C8:48:94:9D:9D:4B:51:C3:FA:4E:D5:0E:54:62:95:94*

Authority Key Identifier *D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*

Certificate Policies

Policy OID: 1.3.6.1.4.1.8149.3.100.2.0

CPS text: [Servidor de Sellado de Tiempo de la Agencia de Tecnología y Certificación Electrónica IVF (Pl. de Napoles y Sicilia 6, CP 46003 CIF Q9650010C). CPS y CP en http://www.accv.es]

CPS pointer: http://www.accv.es/legislacion_c.htm

CRL Distribution Points *http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl*

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2C:8D:42:33:F9:BC:80:93:4E:46:6F:0C:9F:76:41:1F:65:A5:C1:78:98:30:16:0B:66:68:59:EF:93:DE:25:66*

X509SubjectName

Subject C: *ES*

Subject ST: *Valencia*

Subject L: *Valencia*

Subject O: *Agencia de Tecnología y Certificación Electrónica - ACCV*

Subject OU: *PKIACCV*

Subject CN: *TSA1 ACCV 2016*

X509SKI

X509 SK I	*xsTYQMhIlJ2dS1HD+k7VDlRilZQ=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-12-23T02:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

11 - TSP: AC Camerfirma, S.A

.

TSP Name

Name	[en]	*AC Camerfirma, S.A*
Name	[es]	*AC Camerfirma, S.A*

TSP Trade Name

Name	[en]	*VATES-A82743287*
Name	[en]	*Camerfirma*
Name	[es]	*Camerfirma*
Name	[en]	*AC Camerfirma S.A.*
Name	[en]	*AC Camerfirma SA*
Name	[en]	*AC CAMERFIRMA S.A.*

PostalAddress

Street Address	[en]	*C/Ribera del Loira nº12*
Locality	[en]	*Madrid*
State Or Province	[en]	*Madrid*
Postal Code	[en]	*28042*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*C/Ribera del Loira nº12*
Locality	[es]	*Madrid*
State Or Province	[es]	*Madrid*
Postal Code	[es]	*28042*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:info@camerfirma.com*

URI	*[en]*	*http://www.camerfirma.com*

TSP Information URI

URI	*[en]*	*http://www.camerfirma.com/camerfirmaPublic/index/menuf/Ingles.html*
URI	*[es]*	*http://www.camerfirma.com*

11.1 - Service (withdrawn): Qualified Certificates issued by CA AC Racer-2009

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA AC Racer-2009*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Racer - 2009*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIJjCCBg6gAwIBAgIBAzANBgkqhkiG9w0BAQUFADCBqjELMAkGA1UEBhMCRVMxGzAZBgNVBAoT
EkFDIENhbWVyZmlybWEgUy5BLjESMBAGA1UEBRMJQTgyNzQzMjg3MUswSQYDVQQHE0JNYWRyaWQg
KHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgaHR0cHM6Ly93d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVz
cykxHTAhBgNVBAMTFEFDIENhbWVyZmlybWEgLSAyMDA5MB4XDTA5MDMyNTEwNDcwOVoXDTE5MDMy
MzEwNDcwOVowgahxCzAJBgNVBAYTAkVTMR8wGQYDVQQKExJBQyBDYWIlcmZpcm1hIFMuQS4xEjAQ
BgNVBAUTCUE4Mjc0MzI4NzFLMEkGA1UEBxNCTWFkcmlkIChzZWUgY3VycmVudCBhZGRyZXNzIGF0
IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MpMRUwEwYDVQQDEwxSQUNFUiAtIDIw
MDkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDY5FSIYncvISVyf/sMScuTgxo+Uy67
y+UjDPMXc1TYf1aA/UOVZdPI8cB2xt7QnKppMgzo0b4YXi/blAO2OGZTjMYiUQu/8hkF/Cm5
qUFvQR7B/NzAdCgPLiK+P0b2eMNTxqBbsE0K4DujPJ5ykFb4aq3gB66rX2aoABHNBzWZCZQG7x+y
90N1t5EAsyyDjx7J1mSZ9Hgp0rpudtVkpZUlSqJcpau78/D16tH3V8ASA9LH24PoWla53K3je96
E6MR2grg7nL5IADH2Xggstsmgc1rHc/nZ6hDbMNmlcZTPjmEwh9NMH1Z8yzZzKk+AZvOHwleSXs
h5olqRFFX+7LY+P/I/+YEc2cm6+MpvZpJPKqpcVqVz+aLSyumAFvLpXEI7yrv/3xfsm62ykcttSlg
RwDjjaOSUmM8krtJAw3DNwKGkWDaVVmfhRuuCeeUx9fnY+wGP50QPgusJx5n+0ouBn1vrN5WAkp8
Wr++IEHakNVhDen5S1yB/jrfO6krBMc+UCuLKApXOmCQNfg0sX/X7lxyqm1hAL/QTNpasucLQAb
0cS0l1c2f110AD699xOoGfC3nrJTuDpjugqkSLzjKOSAFoXsw266xNUw2cGbcetPc9SlU3J7yUT8
q4UMKvGfde9v/GslsI/+uAUCMXbluIbWURg2R6vee6SEzPdQIDAQABo4ICWzCCAlcwEgYDVR0TAQH/
BAgwBgEB/wIBATAdBgNVHQ4EFgQUrBbXENFvdfaEiGjmRCURcsqzG4AwgdkGA1UdIwSB0TCBzoAU
yAAP/MZS/J/bO2QuMrluLnHzZXmhgbKkga8wgawxCzAJBgNVBAYTAkVVMUMwQQYDVQQHEzpNYWRy
aWQgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MpMRIw
EAYDVQQFEwIBODI3NDMyODcxGzAZBgNVBAoTEkFDIENhbWVyZmlybWEgUy5BLjEnMCUGA1UEAxMe
R2xvYmFsIEloYW1iZXJzaWduIFJvb3QgLSAyMDA4ggECMHoGCCsGAQUFBwEBBG4wbDBCBggrBgEF
BQcwAoY2aHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9hY19jYW1lcmZpcm1hLTIwMDku
Y3J0MCYGCCsGAQUFBzABhhpodHRwOi8vb2NzcC5jYW1lcmZpcm1hLmNvbTAOBgNVHQ8BAf8EBAMC
AQYwPgYDVR0gBDcwNTAzBgRVHSAAMCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vcG9saWN5LmNlbWVy
ZmlybWEuY29tMHoGA1UdHwRzMHEwNqA0oDKGMGidHAtLy9jcmwuY2FtZXJmaXJtYS5jb20vYWNf
Y2FtZXJmaXJtYS0yMDA5LmNybDA3oDWgM4YxaHR0cDovL2NybDEuY2FtZXJmaXJtYS5jb20vYWNf
Y2FtZXJmaXJtYS0yMDA5LmNybDANBgkqhkiG9w0BAQUFAAOCAgEANyeX68TyUP4JUB0WmHMGa8+M
GRuSCK/dgM0NAfCwAOLkxbe+RmdzhMARCraD0MhKOcRJ4O7gG9Htt/g3NronH1CzYnFxlxrC)/hc
7Mud+ZbT+Xz0CY9/8FPBc1tx+ZHLOMTZXZB8lXL/GQJ4b4unciBIOw5MygRQqYA0wLPxMd1oip
35rBLxpmoQML16B1CY8AxJ/ugZMn91mrzbGaZcNrBKo8LsMOzTvhXFHRIsRVEf3A0qDu0jOtoYcA
4yc5x9MZQs7owX/1eIYvY3/qxyi/PcqwsXP4QdOb8fiNbNqjBANyMd3P4mf7BGc2aerhADzyEejC
uwn4dWOw9Q6cSR3IprnN5bog5h9YHFieFJhx1X8dBZhVLA39Ilw/QOgOQ1KOnZj+8/P9th0AJsRn
VPh7NDZqoybGJOncWHwdvY3tF3yz2Z2apJVmEgmM7ovX8U/IR6+zE9wUyYAqmtQI7kuIeecMyt0Nx
m5BEREVJmZ8IT9TAqdhh0eI/h3JLsxxclLhNn9hPomuAw5rsLor4rzYXZTTJ4Za7Kr2ZYNsovt0
rZthW01dPkDb2SZ5NRFSGGlUsgmCRtZlmTVBrJlfE9U5175f64ob4bOXg/S5fNgG8oLudrKPEVnv
5OZ8HE5eDgZaez5s2xECDl/4BYsC/ZYNnWGMv+1nMWkuwp9G2dM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *AC Camerfirma - 2009*

Issuer L: *Madrid (see current address at https://www.camerfirma.com/address)*

Issuer SERIAL NUMBER: *A82743287*

Issuer O:	*AC Camerfirma S.A.*
Issuer C:	*ES*
Subject CN:	*RACER - 2009*
Subject L:	*Madrid (see current address at https://www.camerfirma.com/address)*
Subject SERIAL NUMBER:	*A82743287*
Subject O:	*AC Camerfirma S.A.*
Subject C:	*ES*
Valid from:	*Wed Mar 25 11:47:09 CET 2009*
Valid to:	*Sat Mar 23 11:47:09 CET 2019*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D8:E4:54:88:62:77:2F:89:25:72:7F:FB:0C:E5:EB:93:83:1A:3E:53:2E:BB:CB:E5:23:0C:F3:17:79:32:58:7F:51:1A:03:F2:3F:39:56:5D:3C:8F:1E:07:6C:62:ED:0C:4A:A6:93:20:CF:FA:1B:E1:85:E2:FF:F6:C8:00:ED:8E:19:9D:63:31:88:94:42:E2:7F:F2:12:85:FC:29:B9:A9:41:6F:41:1E:C1:FC:DC:C0:74:28:0F:2E:22:BE:3F:46:F6:78:C3:53:C6:A0:5B:B0:4D:0A:E0:3B:A3:3C:9E:72:90:56:F8:6A:AD:E0:07:AE:AB:5F:66:A8:00:11:CD:07:35:99:09:94:06:EF:1F:B2:F7:43:75:B7:91:00:B3:2C:83:8F:1E:C9:D6:64:99:F4:78:29:D2:BA:6E:6D:DB:55:92:96:54:95:2A:89:7A:96:AE:EF:CF:C3:D7:AB:47:DD:5F:00:48:0F:4B:1F:6E:0F:A1:69:5A:E7:72:B7:8D:EF:7A:13:A3:11:DA:0A:E0:EE:72:F9:94:00:C7:D9:78:20:B2:DB:26:81:C4:EB:1D:CF:ED:9D:9E:A1:0E:13:0D:9A:57:19:4C:F8:E6:13:08:7D:34:C1:F5:67:CC:B3:67:32:A4:F8:06:6F:38:7C:25:79:25:EC:87:9A:25:A9:11:45:5F:EE:CB:63:E3:FF:53:E5:44:7B:67:26:EB:E3:29:66:92:4F:2A:AA:5C:56:A5:73:F9:A2:FC:CA:E9:80:16:F2:E9:8D:71:08:EF:2A:EF:FF:7C:5F:B2:6E:B6:CA:47:2D:AD:22:20:47:00:E3:8D:A3:92:52:63:3C:92:BB:49:03:0D:C3:37:02:86:91:60:DA:55:59:9F:85:1B:AE:09:E7:94:C7:D7:E7:63:EC:06:3F:9D:10:3E:0B:AC:27:1E:67:FB:4A:2E:06:7D:6F:AC:DE:56:02:4A:7C:5A:BF:BE:20:41:DA:90:D5:61:0D:E9:F9:4B:5C:81:FE:3A:DF:3B:AB:64:AC:13:1C:F9:40:AE:2C:A0:29:5C:E9:82:40:D7:E0:D2:C5:FF:5F:B2:31:CA:A9:B5:84:02:FF:41:33:69:6A:CB:9C:2D:00:1B:D1:C4:B4:97:57:36:7F:5D:74:00:3E:BD:F7:13:A8:19:F0:B7:9E:B2:53:B8:3A:63:BA:A8:24:48:BA:E3:28:E4:80:16:85:EC:C3:6E:BA:C4:D5:30:D9:C1:9B:A1:CB:4F:73:D4:A5:53:72:7B:C9:44:FC:AB:85:0C:2A:F1:8E:7B:DB:FF:1A:C9:6C:53:EB:80:50:93:B8:5D:B9:2E:22:15:94:46:0D:91:EA:F7:BA:48:4C:CF:75:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 1*
Subject Key Identifier	*AC:16:D7:10:D1:6F:75:F6:84:88:68:E6:44:25:11:72:CA:B3:1B:80*
Authority Key Identifier	*C8:00:0F:FC:C6:52:FC:9F:DB:3B:64:2E:32:B9:6E:2E:71:F3:65:79*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma-2009.crt* *http://ocsp.camerfirma.com*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma-2009.crl* *http://crl1.camerfirma.com/ac_camerfirma-2009.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*47:CF:DE:E3:76:09:72:5C:FF:03:7B:56:A0:71:C4:3A:A0:58:69:A8:44:28:A5:D8:61:FF:92:B9:45:02:92:AA*

X509SubjectName

Subject CN:	*RACER - 2009*
Subject L:	*Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

11.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	Qualified Certificates issued by CA AC Racer-2009
Name	[es]	Certificados Reconocidos emitidos por la CA Racer - 2009

Service digital identities

X509SubjectName

Subject CN:	RACER - 2009
Subject L:	Madrid (see current address at https://www.camerfirma.com/address)
Subject SERIAL NUMBER:	A82743287
Subject O:	AC Camerfirma S.A.
Subject C:	ES

X509SKI

X509 SK I	rBbXENFvdfaEiGjmRCURcsqzG4A=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Status Starting Time	2016-06-30T22:00:00Z

11.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

11.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA AC Racer-2009*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Racer - 2009*

Service digital identities

X509SubjectName

Subject CN:	*RACER - 2009*
Subject L:	*Madrid (see current address at https://www.camerfirma.com/address)*
Subject SERIAL NUMBER:	*A82743287*
Subject O:	*AC Camerfirma S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*rBbXENFvdfaEiGjmRCURcsqzG4A=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-07-02T00:00:00Z*

11.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.2 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Camerales - 2009

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by the CA Camerfirma Camerales - 2009*

Name *[es]* *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIITjCCBjagAwIBAgIBAjANBgkqhkiG9w0BAQUFADCBrjELMAkGA1UEBhMCRVUxQzBBBgNVBAcT
Ok1hZHJpZCAoc2VlIGN1cnJlbnQgYWRkcmVzcyBhdCB3d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVz
cykxEjAQBgNVBAUTCUE4Mjc0Mzl4NzEbMBkGA1UEChMSQUMgQ2FtZXJmaXJtYSBTLkEuMSkwJwYD
VQQDEyBJaGFtYmVycyBvZiBDb21tZXJjZSBSb290IC0gMjAwODAeFw0wOTAzMTYxNzQwMjBaFw0x
OTAzMTQxNzQwMjBaMIG+MQswCQYDVQQGEwJFUzEbMBkGA1UEChMSQUMgQ2FtZXJmaXJtYSBTLkEu
MRIwEAYDVQQFEwIBODI3NDMyODcxSzBJBgNVBAcTQk1hZHJpZCAoc2VlIGN1cnJlbnQgYWRkcmVz
cyBhdCBodHRwczovL3d3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzKTExMC8GA1UEAxMoQ2FtZXJm
aXJtYSBDZXJ0aWZpY2Fkb3MgQ2FtZXJhbGVzIC0gMjAwOTCCAiIwDQYJKoZIhvcNAQEBBQADggIP
ADCCAgoCggIBAPjxAnnzGKdthBk0aKy/6/z/vUcK0QbDtpokhcm6tLzjSKMiXpfzk0SgvpF4w+c
7XEpPluuoscf5oHtFaWy8tmy3Ma2xCsPQ15/Pf6oGhtK5iEp9fsnjbGM1BkUzzfgemF4bd5Z7
8r3SncXqlXnrbcAWq1mcfNYfVYXEd+weS8ArXtOrx8+b+iODOlYqbhqRcUXdcUzsle4RFVxLnMGr
r7RuoONsbXD2LOu0GLvixac5ABvefsaFmnFxIG4t1yi7h82V9w8QJxak20nYzTOSHUQ1DU32GEBF
N+nF8hvbJ94+6YUb40xQgbVW5qn/50podHiPej1Ei78T29pAooszzA3N4rWuxSMA5Mp9n3ZDXQQ
nMOprn6NUDb4Im4do5sExhD9hBHnzNFPLLFOxUxtBLUfCBkvcZ5gR/mJQ36c9muZQwQyApuhgMqN5
lMgGAIsNNgTQd4rblYD26CC4mBkV5UzCb7ZBsxdm5l06kQgU19pcurSopmJs6NwmzIF9D0nxoLUcJ
wZSD7H6Qqf8MG60bbvxf+r7OxLkzVY8PSDj4E/TY830uZtFYClaE5OBW1S8KpQNlBPzry/aML0tf
o62osFtN9b+EDFcpr2f3qIOrgfBd03CTjEFj4DR8gBF/a2hKn77N8bctx0o+3YiCgqBssqmSTbs1
1toKJcSPAzyDAgMBAAGjggJMIICXzASBgNVHRMBAf8ECDAGAQH/AgECMB0GA1UdDgQWBBQexFqK
hG8RkFizAgnXFubqwyTmj7CB4wYDVR0jBIHbMIHHYgBT5JKwPsrX4ecD6Y1gbxNlNAp4XGaGBtKSB
sTCBrjELMAkGA1UEBhMCRVUxQzBBBgNVBAcTOk1hZHJpZCAoc2VlIGN1cnJlbnQgYWRkcmVzcyBh
dCB3d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzcykxEjAQBgNVBAUTCUE4Mjc0Mzl4NzEbMBkGA1UE
ChMSQUMgQ2FtZXJmaXJtYSBTLkEuMSkwJwYDVQQDEyBJaGFtYmVycyBvZiBDb21tZXJjZSBSb290
IC0gMjAwOTIJAKPaQn6ksa7aMHoGCCSGAQUFBwEBBG4wbDBCBggrBgEFBQcwAoY2aHR0cDov L3d3
dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9yb290X2NoYW1iZXJzL TlwMDguY3J0MCYGCCsGAQUFBzAB
hhpodHRwOi8vb2Nzcc5jYW1lcmZpcm1hLmNvbTAOBgNVHQ8BAf8EBAMCAQYwPgYDVR0gBDcwNTAz
BgRVHSAAMCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vcG9sa WN5LmNhbWVyZmlyb WEuY29tMHgGA1Ud
HwRxMG8wNaAzoDGGL2h0dHA6L y9cmwuY2FtZXJmaXJtYS5jb20v Y2hhbW1cnNvb290L TIwMDgu
Y3JsMDagNKAyhjBodHRwOi8vY3JsMS5jYW1lcmZpcm1hLmNvbS9jaGFtYmVyc3Jvb3QtMjAwOC5j
cmwwDQYJKoZIhvcNAQEFBQADggIBAKs6H/trpHObocHFnFjDFCKs1uVoc5COWe88+V7sBhhtMn5I
9uTXjKMEs7iDLao27+6hJ8G2r1sHGrW5m7Gfg4baABu99evw/j+pKd6S3YiiIBSW0axpitCGLrdh
2gYMLZxMBnoSeIzHiFYc5HWKCrzr2I/Msb9qgOjNEiHVvoEBqcHolJ8Kx59nFJM488XiKzJfc9I
HpD2Xu2cXdjguPaZ7qZEs7KWFNkSSuWTTvSNdm5U9kBSYczzXZ+JEZMtq38exoHPpUQ3GtBVTqpO
wKbluQ+lPm6MC2PzfpZqLr8pS/4iprxjAz/Hl7VuAjAtPRBk1lXAY1aFEkbsPHMOlVHb8mB9AXN9
meUhIj9Hdynx4o14vsBWsYLCF5p1xNOI6b/3ciA21WIzo0umKYg2tPwMKUzadmScQwfMhzimQd
HFjXvMIMpsuwjyNv+GfcxIv2SBiPonvC7TKlibr2lKV2L3yYyR6e2EwpuoKWbfiu2SMNHBrXj2ACF
L+9AqyU2R3gLIP6kSPTLQHwjZe0H1Rv8aFRa4wilMwAgEO+hEklIQ6Ir4JID48QUiAajxEpVMGV1
TsxO6G8kj8tEJMxOS5YHE7b/RjonbNYZLnT9yZt1hMxEwazj5G1SWQNGXJV2cEDcICeuVVMeqBPu
0SWxtw5LeKH2NG+9Gm17Y7zyyRMR

-----END CERTIFICATE-----

Signature algorithm:	*SHA1withRSA*
Issuer CN:	*Chambers of Commerce Root - 2008*
Issuer O:	*AC Camerfirma S.A.*
Issuer SERIAL NUMBER:	*A82743287*
Issuer L:	*Madrid (see current address at www.camerfirma.com/address)*
Issuer C:	*EU*
Subject CN:	*Camerfirma Certificados Camerales - 2009*
Subject L:	*Madrid (see current address at https://www.camerfirma.com/address)*
Subject SERIAL NUMBER:	*A82743287*
Subject O:	*AC Camerfirma S.A.*
Subject C:	*ES*
Valid from:	*Mon Mar 16 18:40:20 CET 2009*
Valid to:	*Thu Mar 14 18:40:20 CET 2019*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:F8:F1:02:79:F3:18:A7:49:B5:B2:24:D1:A2:B2:FF:AF:F3:FE:F5:1C:2B:44:1B:0E:DA:68:92:17:26:EA:D2:F3:8D:22:8C:89:7A:5F:C6:4D:12:82:FA:45:E3:0F:9C:ED:71:29:3E:5B:AE:A2:C7:09:E6:81:C7:7C:56:96:C9:19:B2:DC:CA:36:C4:27:8F:43:5E:7F:FC:F7:FA:A0:68:5F:93:98:84:A7:D2:2C:AA:78:DB:18:CD:65:6E:40:AE:CD:98:1E:98:5E:1B:77:96:7B:F2:BD:D2:9D:C5:EA:95:79:EB:6D:C0:16:AB:59:9C:7C:D6:1F:55:85:C4:77:EC:1E:4B:C0:2B:5E:D3:AB:C7:CF:9B:FA:23:83:3A:D6:2A:6E:1A:91:71:45:DD:71:4C:EC:95:EE:11:15:5C:4B:9C:C1:AB:AF:B4:6E:A0:E3:6C:6D:70:F6:2C:EB:B4:18:BB:E2:C5:A7:39:00:1B:DE:7E:C6:85:9A:71:71:20:6E:2D:D7:28:BB:87:CD:95:F7:0F:10:27:16:A4:DB:49:D8:CD:33:92:1D:44:35:0D:4D:F6:18:40:45:37:E9:C5:F2:1B:DB:27:DE:3E:E9:85:21:E3:4C:50:81:B5:56:E6:A9:FF:FF:9D:29:A1:D1:E2:3D:E8:F5:12:DE:FC:4F:6F:69:02:8A:2C:CD:A0:37:37:8A:D6:BB:14:8C:03:93:29:F6:7D:D9:0D:74:10:9C:C3:A9:AE:7E:8D:50:36:F8:12:62:5D:A3:9B:04:C6:10:CF:85:F1:E6:34:53:CB:2C:53:B1:53:1B:41:2D:48:C2:06:4B:DC:67:98:11:FE:62:50:DF:A7:3D:9A:E6:50:C1:0C:80:A6:E8:60:32:A3:79:94:C8:06:00:8B:0D:36:04:D0:77:8A:DB:95:80:F6:E8:20:B8:98:19:15:E5:4C:C2:6F:B6:41:B3:17:66:E4:8D:3A:91:08:14:D7:DA:5C:BA:B4:A8:A6:62:6C:E8:DC:26:CC:81:7D:0F:49:F1:A1:47:09:C1:94:83:EC:7E:90:A8:FF:0C:1B:A3:9B:86:FC:5F:FA:2E:CE:C4:B9:33:55:8F:0F:48:38:F8:13:F4:D8:F3:7D:2E:66:D1:58:0A:56:84:E4:E0:56:D5:2F:0A:A5:03:65:04:FC:EB:CB:F6:8C:2F:4B:5F:A3:AD:A8:B0:57:CD:F5:BF:84:0C:57:A9:AF:67:F7:A8:83:AB:81:F0:5D:D3:70:93:8C:41:63:E0:34:7C:80:11:7F:6B:68:4A:9F:BE:CD:F1:B7:2D:C7:4A:3E:DD:88:82:82:A0:6C:B2:A9:92:4E:1B:35:D6:DA:0A:22:CE:4F:03:3C:83:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 2*
Subject Key Identifier	*1E:C4:5A:8A:84:6F:11:90:58:B3:E2:09:D7:16:E6:EA:C3:24:E6:8D*
Authority Key Identifier	*F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19*
Authority Info Access	*http://www.camerfirma.com/certs/root_chambers-2008.crt* *http://ocsp.camerfirma.com*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/chambersroot-2008.crl* *http://crl1.camerfirma.com/chambersroot-2008.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *2F:2B:32:E7:8F:C6:9D:2F:FC:64:5E:B6:06:8E:07:4E:74:97:74:49:5F:DC:25:10:93:B0:EE:E0:4E:FA:FD:17*

X509SubjectName

Subject CN: *Camerfirma Certificados Camerales - 2009*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-07-21T00:00:00Z

11.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

11.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by the CA Camerfirma Camerales - 2009*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009*

Service digital identities

X509SubjectName

Subject CN:	*Camerfirma Certificados Camerales - 2009*
Subject L:	*Madrid (see current address at https://www.camerfirma.com/address)*
Subject SERIAL NUMBER:	*A82743287*
Subject O:	*AC Camerfirma S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*HsRaioRvEZBYs+IJ1xbm6sMk5o0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

11.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by the CA Camerfirma Camerales - 2009*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009*

Service digital identities

X509SubjectName

Subject CN:	*Camerfirma Certificados Camerales - 2009*
Subject L:	*Madrid (see current address at https://www.camerfirma.com/address)*
Subject SERIAL NUMBER:	*A82743287*
Subject O:	*AC Camerfirma S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*HsRaioRvEZBYs+IJ1xbm6sMk5o0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-07-02T00:00:00Z*

11.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

11.3 - Service (granted): Qualified Certificates issued by CA AC Camerfirma Certificados Camerales

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA AC Camerfirma Certificados Camerales*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFwDCCBKigAwIBAgIBBTANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJFVTEnMCUGA1UEChMe
QUMgQ2FtZXJmaXJtYSBTQSBDSUYgQTgyNzQzMjg3MSMwIQYDVQQLExpodHRwOi8vd3d3LmNoYW1i
ZXJzaWduLm9yZzEiMCAGA1UEAxMZQ2hhbWJlcnMgb2YgQ29tbWVyY2UgUm9vdDAeFw0wNDAyMDkx
NTQyNDdaFw0zNDAyMDkxNTQyNDdaMIHgMQswCQYDVQQGEwJFUzEuMCwGCSqGSIb3DQEJARYfYWNf
Y2FtZXJmaXJtYV9jY0BjYW1lcmZpcm1hLmNvbTFDMEEGA1UEBxM6TWFkcmlkIChzZWUgY3VycmVu
dCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzKTESMBAGA1UEBRMJQTgyNzQz
Mjg3MRkwFwYDVQQKExBBQyBDYW1lcmZpcm1hIFNBMS0wKwYDVQQDEyRBQyBDYW1lcmZpcm1hIENl
cnRpZmlpYWRvcyBDYW1lcmFsZXMwggEgMA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCjxnvv
j01I36lgGhihRYVf1fAPEXsTJKrY4aLQGEUSh5szZE7VTiGiyMTMc2uCmnaXafjYHK8Lgmy6T9xx
GEZSOS4x6rgtuPyy13APtu3X3Y2kPVLu7ZMw5HoQC64wBj6Ycnx1nBwmVW05DjzRXp6OyBIEKEaA
B9vc2qIJIhY234fGi6Wd/ut1sfDcRZAo+6CSMNQxaY+ryXkD11uWkzWXfa9U2OusG7z4uPqcGr4/
Hz2/CTLDTgp0xkMJYuzOztpUvOACrxlkS2utKUwVIAiKJnboNwf/en94RbHNzkKc5t0SAbzCI57u
cawbzxSdPa+SAC25FNur64FKkfdq5PPjAgEDo4IB5TCCAeEwEgYDVR0TAQH/BAgwBgEB/wIBCzA8
BgNVHR8ENTAzMDGgL6AthitodHRwOi8vY3JsLmNoYW1iZXJzaWduLm9yZy9jaGFrYmVyc3Jvb3Qu
Y3JsMB0GA1UdDgQWBBS2H06dHGiRLjdyYOFGj1qlKjExuTCBqwYDVR0jBIGjMIGggBT7jPWxTenb
oSlbV4tNdgZ24dGiuqGBhKSBgTB/MQswCQYDVQQGEwJFVTEnMCUGA1UEChMeQUMgQ2FtZXJmaXJt
YSBTQSBDSUYgQTgyNzQzMjg3MSMwIQYDVQQLExpodHRwOi8vd3d3LmNoYW1iZXJzaWduLm9yZzEi
MCAGA1UEAxMZQ2hhbWJlcnMgb2YgQ29tbWVyY2UgUm9vdIIBADAOBgNVHQ8BAf8EBAMCAYYwKgYD
VR0RBCMwIYEfYWNfY2FtZXJmaXJtYV9jY0BjYW1lcmZpcm1hLmNvbTAnBgNVHRIEIDAegRxjaGFt
YmVyc3Jvb3RAY2hhbWJlcnNpZ24ub3JnMFsGA1UdIARUMFIwUAYLKwYBBAGBhy4KCQEwQTA/Bggr
BgEFBQcCARYzaHR0cDovL2Nwcy5jYW1lcmZpcm1hLmNvbS9jcHMvYWNfY2FtZXJmaXJtYV9jYy5o
dG1sMA0GCSqGSIb3DQEBBQUAA4IBAQBI8KoPBYL//EBonqQWS0N+hLfxImP1eQ6nac+vR5QtF/0w
+VCTkShKwHan6VWTdPVwXSEC/uvXHkX6DYrtxFGGFB6qxuP1rkIpRssTkAJnvOx3REiFjIkhsi
jKd/jvqxjbMbuYU+EFACK/jQIRoj+LEZ+hauqbALZBIqq26HTqXOitJxsBj6M94YWcfpbTDef
QNWCGsSnZcw2+k+az/wAOZT6xAxlnEimHpDDlgRsmaLrHpDPDoIRYOih0gbJTnn4mKcx9Wgr0sZ+
XFI03j+bvcXL1tiuQnwb9dMRDe/OdXABT35W4ZzLbpost65ZW3Tx+oi/bLbmu6pbKCgs

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *Chambers of Commerce Root*

Issuer OU: *http://www.chambersign.org*

Issuer O: *AC Camerfirma SA CIF A82743287*

Issuer C: *EU*

Subject CN: *AC Camerfirma Certificados Camerales*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *ac_camerfirma_cc@camerfirma.com*

Subject C: *ES*

Valid from: *Mon Feb 09 16:42:47 CET 2004*

Valid to: *Thu Feb 09 16:42:47 CET 2034*

Public Key:

30:82:01:20:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0D:00:30:82:01:08:02:82:01:01:00:A3:C6:7B:EF:8F:4D:5F:DF:A9:60:1A:18:A1:45:85:5F:D5:F0:0F:11:7B:13:24:AA:D8:E1:A2:D0:70:45:12:87:9B:33:6
4:4E:D5:4E:D1:A2:C8:C4:CC:73:6B:82:9A:76:97:69:F8:D8:1C:AF:0B:82:6C:BA:4F:DC:71:18:46:79:39:2E:31:EA:B8:2D:B8:FC:B2:D7:70:0F:B6:ED:D7:DD:8D:A4:3D:52:EE:ED:93:30:E4:7A:10:0B:AE:30:06:3E:98:72:7
C:53:9C:1C:26:55:6D:39:0E:3C:D1:5E:9E:8E:C8:12:04:28:46:80:07:DB:EF:DA:A1:25:7E:1F:D8:DB:7E:05:1B:A5:9D:FE:EB:75:B3:44:9C:45:90:28:FB:A0:92:30:D4:31:69:8F:AB:C9:72:83:D7:5B:96:93:35:97:25:AF:54:64:
E6:AC:1B:BC:F8:B8:FA:9C:1A:BE:3F:3D:BF:09:32:C3:4E:0A:74:C6:43:09:62:EC:CE:CE:DA:54:BC:E0:02:AF:19:64:4B:6B:AD:29:4C:15:94:08:A4:26:76:E8:37:07:FF:7A:7F:78:45:B1:CD:CE:42:9C:E6:DD:12:01:BC:
C2:7F:9E:EE:79:AC:1B:CF:14:9D:3D:AF:92:00:2D:B9:14:DB:AB:EB:81:4A:91:F7:6A:E4:F3:E3:02:01:03

Basic Constraints *IsCA: true - Path length: 11*

CRL Distribution Points *http://crl.chambersign.org/chambersroot.crl*

Subject Key Identifier *B6:1F:4E:9D:1C:68:91:2E:37:72:60:E1:46:8F:5A:A5:2A:31:31:B9*

Authority Key Identifier *E3:94:F5:B1:4D:E9:DB:A1:29:5B:57:8B:4D:76:06:76:E1:D1:A2:8A*

Subject Alternative Name *ac_camerfirma_cc@camerfirma.com*

Issuer Alternative Name *chambersroot@chambersign.org*

Certificate Policies *Policy OID: 1.3.6.1.4.1.17326.10.9.1*

CPS pointer: http://cps.camerfirma.com/cps/ac_camerfirma_cc.html

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C7:D8:43:81:E1:1F:7C:57:46:77:1A:F5:B0:50:DC:51:FC:6F:DA:D6:F6:F3:5B:B5:3A:3D:E9:13:82:2E:A0:9E*

X509SubjectName

Subject CN: *AC Camerfirma Certificados Camerales*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *ac_camerfirma_cc@camerfirma.com*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-06-09T00:00:00Z

11.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

11.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.3.3 - History instance n.1 - Status: withdrawn

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by CA AC Camerfirma Certificados Camerales
Name	[es]	Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales

Service digital identities

X509SubjectName

Subject CN:	AC Camerfirma Certificados Camerales
Subject O:	AC Camerfirma SA
Subject SERIAL NUMBER:	A82743287
Subject L:	Madrid (see current address at www.camerfirma.com/address)
Subject E:	ac_camerfirma_cc@camerfirma.com
Subject C:	ES

X509SKI

X509 SK I	th9OnRxokS43cmDhRo9apSoxMbk=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Status Starting Time 2017-07-21T00:00:00Z

11.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

11.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.3.4 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by CA AC Camerfirma Certificados Camerales

Name [es] Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales

Service digital identities

X509SubjectName

Subject CN: AC Camerfirma Certificados Camerales

Subject O: AC Camerfirma SA

Subject SERIAL NUMBER: A82743287

Subject L: Madrid (see current address at www.camerfirma.com/address)

Subject E: ac_camerfirma_cc@camerfirma.com

Subject C: *ES*

X509SKI

X509 SK I *th9OnRxokS43cmDhRo9apSoxMbk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.3.4.3 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

11.3.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.3.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA AC Camerfirma Certificados Camerales*

Name [es] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

Service digital identities

X509SubjectName

Subject CN: *AC Camerfirma Certificados Camerales*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *ac_camerfirma_cc@camerfirma.com*

Subject C: *ES*

X509SKI

X509 SK I *th9OnRxokS43cmDhRo9apSoxMbk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

11.3.5.5 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

11.4 - Service (withdrawn): Qualified Certificates issued by CA AC Racer

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by CA AC Racer*

Name *[es]* *Certificados Reconocidos emitidos por la CA Racer*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGDzCCBPegAwIBAgIBATANBgkqhkiG9w0BAQUFADCBxjELMAkGA1UEBhMCRVMxKzApBgkqhkiG
9w0BCQEWHGFjX2NhbWVyZmlybWFAY2FrZXJmaXJtYS5jb20xEjAQBgNVBAUTCUE4Mjc0Mzl4NzFD
MEEGA1UEBxM6TWFkcmlkIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZpcm1hLmNv
bS9hZGRyZXNzKTEZMBcGA1UEChMQQUMgQ2FrZXJmaXJtYSBTQTEWMBQGA1UEAxMNQUMgQ2FrZXJm
aXJtYTAeFw0wMzEyMDQxNzI2NDFaFw0yMzEyMDQxNzI2NDFaMIG4MQswCQYDVQQGEwJFUzElMCMG
CSqGSIb3DQEJARYWY2FyYWNlckBjYW1lcmZpcm1hLmNvbTFDMEEGA1UEBxM6TWFkcmlkIChzZWUg
Y3VycmVudCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzKTESMBAGA1UEBRMJ
Q1gyNzQzMjg3MRkwFwYDVQQKExBBQyBDYW1lcmZpcm1hIFNBMQ4wDAYDVQQDEwVSQUNFUjCCAR8w
DQYJKoZIhvcNAQEBBQADggEMADCCAQcCggEAe03yv1HZxgtdg1b2NocXqtM73x6992kg9feecE3t
36NAdYmy+ob6MkrT3CfQfGHLmr+RyyadD6o0D0LNcGrRYpcFw7ZtOYX/mMGTIXKLPka7BdoCygyx
4amyBigZV6AjGn4+xIzQy5ljOyVlnfFtI49awkfX0+BNv5qWKpshg+WnFOW1Gd0MIXMH6uNsu2/H
dqSgsvUQ1dQNelKxz+EbTfiuw+HwgQbpf/nsc4oGv0cq0pA85gdEoO+lLOwRZ8DOfAaVYATnqfTv
YcxwYYcQ7NWDxCX05Vs51rbt5Qrwlq/St7L/6xQd++0mlfAJoC7TF5Csagh2uS5KSMgf9WPwwIB
A60CAbUwggIRMBIGA1UdEwEB/wQIMAYBAf8CAQowNAYDVR0fBC0wKzApoCegJYYjaHR0cDovL2Ny
bC5jYW1lcmZpcm1hLmNvbS9yYWNlci5jcmwwHQYDVR0OBBYEFL68CNQuugBMgNwmZ7Sl2N3DShr5
MIGoBgNVHSMEgaAwgZ2AFHDBlfpdpRa+YuikfePUZF/E4T6doYGBpH8wTELMAkGA1UEBhMCRVUx
JzAlBgNVBAoTHkFDIENhbWVyZmlybWEgU0EgQ0lGIEE4Mjc0MzI4NzEjMCEGA1UECxMaaHR0cDov
L3d3dy5jaGFrYmVyc2lnbi5vcmcxID AcBgNVBAMTF0dzb2lhbCBlbGFrYmVyc2lnbiBSb290ggEC
ME0GCCsGAQUFBwEBBEEwPzA9BggrBgEFBQcwAoYxaHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9j
ZXJ0cy9hY19jYW1lcmZpcm1hLmNydDAOBgNVHQ8BAf8EBAMCAYYwIQYDVR0RBBowGIEWY2FyYWNl
ckBjYW1lcmZpcm1hLmNvbTAnBgNVHRIEIDAegRxbY19jYW1lcmZpcm1hQGNhbWVyZmlybWEuY29y
MFAGA1UdIARJMEcwRQYLKwYBBAGIBy4KCAEwNjA0BggrBgEFBQcCARYoaHR0cDovL2Nwcy5jYW11
cmZpcm1hLmNvbS9jcHMvcmFjZXIuaHRtbDANBgkqhkiG9w0BAQUFAAOCAQEAVPqOALDxl2F8rgu6
7OcqomMXR3aPlyFE4mFeKOzVpQFsRRzkls3c1ZDTGYlVb9XnL4AIBJ/U1ukRkGulZHIYUWiNADWd
0HImPb5Hzgup0R9dNXP2SrSo4d2iB7gqR86X1t3bjdf152PuCm/tE6sImR13VqKmjSd1sYxTNAKc
Pu31YDZgGLnNFd3qN2QbPWq69Z/1q+7L7a15TXcBNQXsfQEOLGx5t9ZcNDVmpSH06swHO3Gql2n
/qNuNHgbw7+QZZZJfarv2ArgMCU2SnnpCmpybtruKwGbelQHYC2oJavTHoLd5GeIH4GtvPIE9cxhz
f8XjZXECKL54a/4o9ISBcA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *AC Camerfirma*

Issuer O: *AC Camerfirma SA*

Issuer L: *Madrid (see current address at www.camerfirma.com/address)*

Issuer SERIAL NUMBER: *A82743287*

Issuer E: *ac_camerfirma@camerfirma.com*

Issuer C: *ES*

Subject CN: *RACER*

Subject O:	*AC Camerfirma SA*
Subject SERIAL NUMBER:	*A82743287*
Subject L:	*Madrid (see current address at www.camerfirma.com/address)*
Subject E:	*caracer@camerfirma.com*
Subject C:	*ES*
Valid from:	*Thu Dec 04 18:26:41 CET 2003*
Valid to:	*Mon Dec 04 18:26:41 CET 2023*
Public Key:	*30:82:01:1F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0C:00:30:82:01:07:02:82:01:00:7B:4D:F2:CB:51:D9:C6:0B:5D:83:56:F6:36:87:17:AA:D3:3B:DF:1E:BD:F7:69:20:F5:F7:9E:70:4D:ED:DF:A3:40:75:89:B2:FA:88:7A:30:AA:D3:DC:22:10:46:21:CB:9B:EF:D1:CB:2B:9D:0F:AA:34:0F:42:CD:78:6A:D1:62:97:05:C3:BC:C4:39:85:FF:98:C1:93:21:72:8B:3E:4B:BB:05:DA:02:BE:0C:B1:E1:A9:B2:06:28:19:57:A0:23:1A:7E:3E:C4:8C:D0:CB:99:63:3B:25:65:9D:F1:5F:23:8F:5A:C2:47:D7:D3:E0:4D:BF:9A:96:2A:9B:21:83:E5:A7:14:E5:B5:19:DD:0C:25:73:07:EA:E3:6C:BB:6F:C7:76:A4:A0:B2:F5:10:D5:D4:0D:7A:52:B1:CF:E1:1B:4D:F8:AE:C3:E1:F0:81:06:E9:7F:F9:EC:7B:8A:06:BF:47:2A:D2:90:3C:E6:07:44:A0:EF:9F:2C:EC:11:67:C0:CE:7C:06:95:60:04:E7:A9:F4:EF:61:EC:70:61:87:10:EC:D5:83:C4:25:F4:E6:25:6C:E7:5A:DB:B7:94:2B:C0:8A:BF:4A:DE:CB:FF:AC:50:77:EF:B4:9A:57:C0:26:80:BB:4C:5E:42:6A:CA:A1:DA:E4:B9:29:23:20:23:D5:8F:C3:02:01:03*
Basic Constraints	*IsCA: true - Path length: 10*
CRL Distribution Points	*http://crl.camerfirma.com/racer.crl*
Subject Key Identifier	*BE:BC:08:D4:2E:BA:00:4C:80:DC:26:67:B4:A5:D8:DD:C3:4A:1A:F9*
Authority Key Identifier	*70:C1:95:FA:5D:A5:16:BE:62:E8:A4:7D:E3:D4:64:5F:C4:E1:3E:9D*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma.crt*
Subject Alternative Name	*caracer@camerfirma.com*
Issuer Alternative Name	*ac_camerfirma@camerfirma.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.17326.10.8.1* *CPS pointer: http://cps.camerfirma.com/cps/racer.html*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F1:71:21:77:93:5D:BA:40:BD:BD:99:C5:F7:53:31:9C:F6:29:35:49:B7:28:47:41:E4:39:16:AD:3B:FB:DD:75*

X509SubjectName

Subject CN:	*RACER*
Subject O:	*AC Camerfirma SA*
Subject SERIAL NUMBER:	*A82743287*
Subject L:	*Madrid (see current address at www.camerfirma.com/address)*

Subject E: *caracer@camerfirma.com*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

11.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA AC Racer*

Name [es] *Certificados Reconocidos emitidos por la CA Racer*

Service digital identities

X509SubjectName

Subject CN: *RACER*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *caracer@camerfirma.com*

Subject C: *ES*

X509SKI

X509 SK I *vrwI1C66AEyA3CZntKXY3cNKGvk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA AC Racer*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Racer*

Service digital identities

X509SubjectName

Subject CN:	*RACER*
Subject O:	*AC Camerfirma SA*
Subject SERIAL NUMBER:	*A82743287*
Subject L:	*Madrid (see current address at www.camerfirma.com/address)*
Subject E:	*caracer@camerfirma.com*
Subject C:	*ES*

X509SKI

X509 SK I	*vrwI1C66AEyA3CZntKXY3cNKGvk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-07-02T00:00:00Z*

11.4.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.5 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Public Administration

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by the CA Camerfirma Public Administration*

Name *[es]* *Certificados Reconocidos emitidos por la CA Camerfirma AAPP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *13*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGaTCCBVGgAwIBAgIBDTANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJFVTEnMCUGA1UEChMe
QUMgQ2FiZXJmaXJtYSBTQSBDSUYgQTgyNzQzMjg3MSMwIQYDVQQLExpodHRwOi8vd3d3LmNoYW1i
ZXUzaWduLm9yZzEzMCAGA1UEAxMZQ2hhbWlzaWduZmgb2YgQ29bWVyY2UgUm9vdDAzEwt0xMDAyMjMw
ODQ2MzdaFw0yMjAyMjAwODQ2MzdaMIGwMQswCQYDVQQGEwJFUzEfMBkGA1UEChMSQUMgQ0FNRVJG
SVJNQSBTLkEuMTswOQYDVQQHEzJNQURSSUQgKFZlciBlbiBodHRwczovL3d3dy5jYW1lcmZpcm1h
LmNvbS9hZGRyZXNzKTEWMBQGA1UECxMNQUMgQ0FNRVJGSVJNQTESMBAGA1UEBRMJQTgyNzQzMjg3
MRswGQYDVQQDExJBQyBDQUlFUkZUIUk1BIEFBUFAwggEgMA0GCSqGSIb3DQEBAQUAA4IBDQAwggEI
AoIBAQDcNq5DM3X0DUeai9Ks7lY6imhlO3vifimirtDdlCkoomMhFq7oE9Q6X5lko95+mpClRm/n
D1XqBOTa04WAYyverGXRH0F6vElp86ew3I8CLUtWdeG255m2xcCcSKOreGDdcd/z+Usgdauerhvb
JG1CmbAr1oWlmVCvr9zN2Frm9NvkFespl8TKkAAXHkza5yuC2SmTXH6LWxTCm03kifVlRpl/329
JdNRRGjtgj+yTHqtgS0TDZ9Snu3yKn/s+KwqK9J+uUHWqgOmEghrYTpzXCGEpPv2TyEAXOhszX
3vzNwStgf8Slz9d4H1TfEsUh02bmXb7e8G5UuybNY0vNAgEDo4ICvjCCArowEgYDVR0TAQH/BAgw
BgEB/wIBAjBuBgNVHR8EZzBlMDCgLqAshipodHRwOi8vY3JsLmNhbWVyZmlybWEuY29tL2NoYW1iZXJzcm9v
ZXJzcm9vdC5jcmwwMaAvoC2GK2h0dHA6Ly9jcmwxLmNhbWVyZmlybWEuY29tL2NoYW1iZXJzcm9v
dC5jcmwwHQYDVR0OBBYEFOVGUOhDoLL3HOS2/9gABCD3H6QLMIGrBgNVHSMEgaMwgaCAFOOU9bFN
6duhKVtX6012Bnb0uKKoYGEpIGBMH8xCzAJBgNVBAYTAkVYMScwJQYDVQQKExSBQyBDYWI1cmZp
cm1hIFNBIENJRiBBODI3NDMyODcxIzAhBgNVBAsTGmh0dHA6Ly93d3cuY2hbbWJlcnNpZ24ub3Jn
MSIwIAYDVQQDExlDaGFtYmVycyBvZiBDb21lZXJjZSBSb290ggEAMHUGCCsGAQUFBwEBBGkwZzA9
BggrBgEFBQcwAoYxaHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9yZX0lcy9ST09UL1NiQU1CRVJT
LmNvdDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3AuY2FlZXJmaXJtYS5jb20wDgYDVR0PAQH/BAQD
AgEGMAkGA1UdEQQCMAAwJwYDVR0SBCAwHoEcY2hhbWJlcnNyb290QGNoYW1iZXJzaWduLm9yZzCB
qwYDVR0gBIGjMIGgMIGdBgsrBgEEAYGHLgEDATCBjTApBggrBgEFBQcCARYdaHR0cHM6Ly9wb2xp
Y3kuY2FlZXJmaXJtYS5jb20wYAYIKwYBBQUHAgIwVBpSQ2VydGlmaWNhZG8gcmHtei4gQ29uc3Vs
dGU;gbGFzIGNvbmRpY2lvbmVzIGRlIHVzbyBlbiBodHRwczovL3Bvb2ljes5jYW1lcmZpcm1hLmNv
bTANBgkqhkiG9w0BAQUFAAOCAQEADuarT/NOdigXhtxzdHZQOjpbY8s/ED8oeSGCil8vypvYJhGL
Q+NDrIl4wXOm/gPJ+fU3YUndDiL5FIi2ld4nch+b8pFes5MIXqSVPsEdi4jWYMh73x8bEDTGO+Fn
zxtgVW+/g5V9sYlJ3tr9CtRVBoCyJ2ADUb35hFoBAxHJkj2G5aPoDFNZUCbkTvQKaUFh920JNaDx
vjS/Kx+ICG8dsUHoiYLZ6ZdC4ltIAtOIgXw5zAkdv757YSq57OTMW3pjNXwHjaOVznyZc8jNNlW4
dpcfTN+udKyeoZEEklGgVs2w72Dw4D7ji2xAvhNieH+uwl8XMLV1Ck48tHn5NpLFng==

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA1withRSA*
Issuer CN:	*Chambers of Commerce Root*
Issuer OU:	*http://www.chambersign.org*
Issuer O:	*AC Camerfirma SA CIF A82743287*
Issuer C:	*EU*
Subject CN:	*AC CAMERFIRMA AAPP*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA*
Subject L:	*MADRID (Ver en https://www.camerfirma.com/address)*
Subject O:	*AC CAMERFIRMA S.A.*
Subject C:	*ES*
Valid from:	*Tue Feb 23 09:46:37 CET 2010*
Valid to:	*Sun Feb 20 09:46:37 CET 2022*
Public Key:	*30:82:01:20:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0D:00:30:82:01:08:02:82:01:01:00:DC:36:AE:43:33:75:F4:0D:47:9A:8B:D2:AC:EE:56:3A:8A:29:A1:20:ED:EF:89:F9:A2:9E:B0:DD:94:29:28:A2:63:21:16:AE:E8:13:D4:3A:5F:99:64:A3:DE:7E:9A:90:A5:46:6F:E7:0F:55:EA:04:E4:DA:D3:85:80:63:2B:DC:AC:65:D1:1F:41:7A:BC:42:29:F3:A7:B0:DC:8F:02:2D:4B:56:75:E1:B6:E7:99:B6:C5:C0:9C:48:A3:AB:78:60:DD:71:DF:F3:F9:4B:20:75:AB:9E:AE:1B:DB:24:6D:42:99:B0:2B:D6:85:A5:99:50:AF:AF:DC:CD:D8:5A:E7:F4:DB:E4:17:F7:AC:A5:FF:13:2A:40:00:5C:7F:33:6B:9C:AE:0B:68:B9:99:35:C7:E8:B5:B1:4C:29:B4:DE:47:EB:54:94:69:53:7D:BD:25:D3:51:44:81:A3:B6:08:FE:C9:31:EA:8A:0E:74:4C:36:7D:4A:7B:B7:C8:A9:FF:B3:E2:B0:A8:AF:65:FB:05:07:21:6A:A0:3A:61:20:86:B6:13:8F:35:C2:18:4A:4F:BF:64:F2:10:05:CE:86:CC:D7:DE:FC:CD:C1:2B:60:7F:C4:A5:CF:D7:78:1F:54:DF:12:C5:21:D3:66:E6:5D:BE:DE:F0:6E:54:BB:26:CD:63:4B:CD:02:01:03*
Basic Constraints	*IsCA: true - Path length: 2*
CRL Distribution Points	*http://crl.camerfirma.com/chambersroot.crl* *http://crl1.camerfirma.com/chambersroot.crl*
Subject Key Identifier	*E5:46:50:E8:43:A0:B2:F7:1C:E4:B6:FF:D8:00:04:20:F7:1F:A4:0B*
Authority Key Identifier	*E3:94:F5:B1:4D:E9:DB:A1:29:5B:57:8B:4D:76:06:76:E1:D1:A2:8A*
Authority Info Access	*http://www.camerfirma.com/certs/ROOT-CHAMBERS.crt* *http://ocsp.camerfirma.com*
Subject Alternative Name	*[]*
Issuer Alternative Name	*chambersroot@chambersign.org*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.17326.1.3.1* *CPS pointer: https://policy.camerfirma.com* *CPS text: [Certificado raíz. Consulte las condiciones de uso en https://policy.camerfirma.com]*
Key Usage:	*keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *83:90:E7:03:57:E9:B5:73:CA:3D:D2:9D:BD:DC:23:7E:CA:F9:36:78:2C:A3:38:9C:79:43:FB:C2:B7:FA:A0:B6*

X509SubjectName

Subject CN: *AC CAMERFIRMA AAPP*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA*

Subject L: *MADRID (Ver en https://www.camerfirma.com/address)*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-07-21T00:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

11.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

11.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.5.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Public Administration

Name [es] Certificados Reconocidos emitidos por la CA Camerfirma AAPP

Service digital identities

X509SubjectName

Subject CN: AC CAMERFIRMA AAPP

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA

Subject L: MADRID (Ver en https://www.camerfirma.com/address)

Subject O: AC CAMERFIRMA S.A.

Subject C: ES

X509SKI

X509 SK I 5UZQ6EOgsvcc5Lb/2AAEIPcfpAs=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

11.5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

11.5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.5.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Public Administration

Name [es] Certificados Reconocidos emitidos por la CA Camerfirma AAPP

Service digital identities

X509SubjectName

Subject CN: AC CAMERFIRMA AAPP

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA

Subject L: MADRID (Ver en https://www.camerfirma.com/address)

Subject O: AC CAMERFIRMA S.A.

Subject C: ES

X509SKI

X509 SK I 5UZQ6EOgsvcc5Lb/2AAEIPcfpAs=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2010-07-22T00:00:00Z

11.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

11.6 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014*
Name	*[es]*	*Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1533704735413519034*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIhzCCBm+gAwIBAgIIFUjQVLioQrowDQYJKoZIhvcNAQELBQAwga4xCzAJBgNVBAYTAkVVMUMw
QQYDVQQHEzpNYWRyaWQgKHNlZSBjaXJvZW50IGFkZHIlc3MgYXQgd3d1LmNhbWVyZmlybWEuY29t
L2FkZHIlc3MpMRIwEAYDVQQFEwlBODI3NDMyODcxGzAZBgNVBAoTEkFDIENhbWVyZmlybWEgUy5B
LjEpMCcGA1UEAxMgQ2hhbWllcnMgb2YgQ29tbWVyY2UgUm9vdCAtIDIwMDgwHhcNMTQxMjE2MTE1
OTAxWhcNMzcxMjE1MTE1OTAxWjCBxzELMAkGA1UEBhMCRVMxFjAUBgNVBAsMDUFDIENBT1VSRkIS
TUExGzAZBgNVBAoMEkFDIENhbWVyZmlybWEgUy5BLjESMBAGA1UEBRMJOTgyNzQzMjg3MUswSQYD
VQQHDEJNYWRyaWQgKHNlZSBjaXJvZW50IGFkZHIlc3MgYXQgaHR0cHM6Ly93d3cuY2FlZXJmaXJt
YS5jb20vYWRkcmVzcykxIjAgBgNVBAMMGUNhbWVyZmlybWEgQUFQUCBJSSAtIDIwMTQwggIiMA0G
CSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDF+2P268Q6GbrsF+dNK9AZI7nvEHs6MSs0gbPCQt4i
/psWIrahzNwdJsjuJzY7n6kRe0d2DEKgo854sNt+G0b0Zyy6gx++NqnRwEIDwg/CR214Zd9TVpIW
ZA0KhDDBRu0EdIDzUi3/vhtLt0Kcx+aYt+WJ5pNUaNMdYe7MK1CaIKFCWbX69KfNPLa6saZiEYSij
D0l9JCU09bN2cVidW/ZsDVR5+Znz6z+tQFXIzSwRebT2uEFDc1SNiB4jZ09n83CALULZPWm1JfUG
Ycei+nQA2ZKZZSZgmmrqsHTUVqC2IzVxkCbxY8vWFyAiE7wkV1S31PBE8AjDYOqi0fRPwWOId+G8
qp0Wo9ofMEBZvwIDEkOBz1vLzo69lOKIxQyPbdbRUvkfvOQoiM0phssbH3HjgqYhs7XrMDTeZKXN
X1As8gf922KWRWbPQ1nSHUWTmxY5KCSAVp8Oj b9xuSzRqJM0+/5AcfBwIqIxdscZZUWNIYbXm
ciHmEzhYzcD2WILmMjuJQtGXz0cNllkqXxqCHhtR+hjnipIEcdOFhVHB5h/SnfAvN7zARl6yZeQ5
bwoQG7s8DPhXCwNJAD91FTCq2sovjpeoMQhACBvTJNy9uhkxIxw7eEHJzSbPr12izAtcJr3QbGiw
fZuJBk4MRhHOSs2fcE58PcukvPz7utd9wIDAQABo4ICjDCCAogwEgYDVR0TAQH/BAgwBgEB/wIB
AjAdBgNVHQOEFgQUXaFVpNxKrIMR+aoS5doSvVFUwwgeMGA1UdIwSB2CB2IAU+SSsD7K1+HnA
+mCIG8TZTQKeFxmhgbSkgbEwga4xCzAJBgNVBAYTAkVVMUMwQQYDVQQHEzpNYWRyaWQgKHNlZSBj
dXJyZW50IGFkZHIlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHIlc3MpMRIwEAYDVQQFEwlB
ODI3NDMyODcxGzAZBgNVBAoTEkFDIENhbWVyZmlybWEgUy5BLjEpMCcGA1UEAxMgQ2hhbWllcnMg
b2YgQ29tbWVyY2UgUm9vdCAtIDIwMDdCCQCZ2kJ+pLGu2jB6BggrBgEFBQcBAQRuMGwwQgYIKwYB
BQUHMAKGNmh0dHA6Ly93d3cuY2FlZXJmaXJtYS5jb20vY2VvdHMvcm9vdF9jaGFlYmVycyfbyMDA4
LmNydDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3Au Y2FlZXJmaXJtYS5jb20wDgYDVR0PAQH/BAQD
AgEGMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYIKwYBBOUHAwEwPgYDVR0gBDcwNTAz
BgRVHSAAMCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vcG9saWNSLmNhbWVyZmlybWEuY29tMHgGA1Ud
HwRxMG8wNaAzoDGGL2h0dHA6L y9rcmwuY2FlZXJmaXJtYS5jb20v Y2hhbWllcnNvb290L TlwMDgu
Y3JsMDagNKAyhjBodHRwOi8vY3JsMS5jYW1lcmZpcm1hLmNvbS9jaGFlYmVyc3Jvb3QtMjAwOC5j
cmwwDQYJKoZIhvcNAQELBQADggIBACVw1zHgpXsOIY2e9OTKHwhrzkM1b1hQB+ZXgmjcxnCy0MmC
WtK2hs1ydBXzMp/CGXEXGK/pcp8VZO5DA+k9yJnRZzU/0PRcHbQVwU1ID923GmKyi7cjVlts7OIm
GY2cg7Zod8dIXiTB1Yy2mmacPovehyzxwQJx7dAV0bctHIlc1Ins4YMUiY3ot+uopPBi7PnJ/TE
iCb6j9un5jpXIf5HpaVGpQCv1l+jnx8n2gxcGGbHLYdyrBnLWS96g1IQkRgXXES5pTy8YUXJM4tN
dIP36pAMjXidwPQcXj/IshdG7mHnxqYBtiYiNOgdxOnZRqILOhN9ObVtKANUUkQcNh1Q2B3PNLHY
Rgkay7oQn2q6MY7xW0PNY5vlhTb2h71Y06deKLSbz82/8hqZU/swIPQF00njcJOhxq7GxMEgTE
AtvmdXVcVNsVzFiux6UPbXYkWXb0cbr+cTpKq6vMvSbp7UOxPtpWmIhIhjHK0LKD+cBILrpvGw
dTTpJ9r9oW/83z+6c1DGVpsZ+GiuemLqfpqUhsIn0tebS1yDH8RNVY18UXkSv13Cea3BLdb/y5rP
obu1GkRJwV+Iyt3mSOkE1pRDqCyx14PnZdsBtHlw/KmqqRdONOjmkaxgcp+uvs/z4SJPn6GrY21i
wU5qXxCaqaE4ysZEp8L0t9xGbbIB

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Chambers of Commerce Root - 2008*

Issuer O: *AC Camerfirma S.A.*

Issuer SERIAL NUMBER: *A82743287*

Issuer L: *Madrid (see current address at www.camerfirma.com/address)*

Issuer C: *EU*

Subject CN: *Camerfirma AAPP II - 2014*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

Valid from: *Tue Dec 16 12:59:01 CET 2014*

Valid to: *Tue Dec 15 12:59:01 CET 2037*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C5:FB:63:F6:EB:C4:3A:19:BA:EC:7F:E7:4D:2B:D0:19:23:B9:EF:10:7B:3A:31:2B:34:81:B3:DC:42:DE:22:FE:9B:16:D6:B6:A1:CC:DC:1D:7E:C8:EE:27:36:3B:9F:A9:11:7B:47:76:0E:45:E0:A3:CE:78:B0:DB:7E:1B:46:F4:67:2C:BA:83:1F:BE:36:AA:6D:47:01:03:C2:0F:C2:47:6D:78:D9:DF:53:56:99:56:64:0D:0A:84:30:C1:46:E3:84:74:3C:D4:DF:FE:6F:86:D2:ED:3B:C7:31:F9:A6:2D:F9:62:79:A4:D5:1A:34:C7:58:7B:B3:0A:D4:26:89:28:50:96:6D:7E:BD:25:D3:4F:51:AD:2C:69:98:84:61:28:A3:0F:49:7D:24:25:34:F6:13:76:71:58:9D:5B:F6:6C:0D:54:79:F9:99:F3:EB:3F:A2:40:55:DF:CD:2C:11:79:B4:F6:B8:41:43:73:54:8D:88:1E:23:67:4F:67:F3:70:80:2D:42:D9:3D:69:B5:25:F5:06:61:C7:A2:FA:74:00:D9:92:99:65:26:60:9A:6A:EA:B0:74:D4:56:A0:B6:27:35:71:90:26:F1:63:CB:D6:17:20:22:13:BC:24:57:54:B7:D4:F0:44:F0:08:C3:60:EA:A2:D1:F4:4F:C1:63:9F:77:E1:BC:AA:9D:16:A3:DA:1F:30:40:59:BF:0F:C3:12:43:81:CF:5B:CB:CE:8E:BD:94:E2:A5:C5:0C:8F:6D:D6:D1:52:F9:1F:BC:E4:28:88:CD:29:86:CB:1B:1F:71:FF:82:A6:21:B3:B5:EB:30:34:DE:64:A5:CD:5F:50:2C:06:07:FD:DB:62:96:45:66:CF:43:59:F8:48:75:16:4E:6C:58:7F:92:82:48:05:69:04:E8:C8:F7:2C:6E:E7:34:6A:94:CD:3E:FF:90:1E:20:1C:08:A8:8C:5D:B1:E6:59:51:63:48:61:B5:E6:72:21:E6:13:38:38:CD:E0:F6:58:82:E6:32:3B:89:42:21:97:CF:47:0D:94:89:2A:5F:1A:82:1E:1B:51:FA:18:E7:8A:9B:44:71:D3:85:85:51:C1:E6:1F:D2:9D:F0:2F:37:BC:C0:46:5E:B2:65:E4:39:6F:0A:10:1B:BB:3C:0C:F8:57:0B:03:49:00:3F:75:15:30:AA:DA:CA:2F:8E:97:A8:31:08:40:08:1B:D3:24:DC:BD:BA:19:31:23:1C:3B:78:41:C9:CD:26:CF:AF:5D:A2:CC:0B:5C:26:BD:D0:6C:68:B0:7D:96:89:06:4E:0C:46:1F:C7:39:2B:36:7D:E1:39:F0:F7:2E:92:F3:F3:EE:EB:5D:F7:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *5D:A1:55:A4:DC:4A:AC:83:11:F9:AA:38:E5:F7:68:4A:FE:15:15:4C*

Authority Key Identifier *F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19*

Authority Info Access	*http://www.camerfirma.com/certs/root_chambers-2008.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth - id_kp_serverAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/chambersroot-2008.crl* *http://crl1.camerfirma.com/chambersroot-2008.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*72:39:D2:F7:70:FA:FF:3B:1C:F8:BE:2A:05:EC:03:ED:EA:AC:05:3B:55:4F:90:D3:69:21:15:5B:A8:05:19:81*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

11.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

11.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.6.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014

Name [es] Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014

Service digital identities

X509SubjectName

Subject CN: Camerfirma AAPP II - 2014

Subject L: Madrid (see current address at https://www.camerfirma.com/address)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject OU: AC CAMERFIRMA

Subject C: ES

X509SKI

X509 SK I XaFVpNxKrIMR+ao45fdoSv4VFUw=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

11.6.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

11.6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.6.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014

Name [es] Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014

Service digital identities

X509SubjectName

Subject CN: Camerfirma AAPP II - 2014

Subject L: Madrid (see current address at https://www.camerfirma.com/address)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject OU: AC CAMERFIRMA

Subject C: ES

X509SKI

X509 SK I XaFVpNxKrIMR+ao45fdoSv4VFUw=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2015-07-07T00:00:00Z

11.6.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

11.7 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *8837493713140842243*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJVzCCBz+gAwIBAgIEqUVtYSBwMwDQYJKoZIhvcNAQELBQAwgfIxCzAJBgNVBAYTAkVTMQ8w
DQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BREJURDE6MDgGA1UECwwxc2VlIGN1cnJlbnQgYWRk
cmVzcyBhdCB3d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzczEpMCcGA1UECwwgQ0hBTUJFUlMgI0Yg
Q09NTUVSQ0UgUk9PVCAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0MzHNzEbMBkGA1UECgwSQUMgQ0FN
RVJGSVJNQSBTLkEuMSkwJwYDVQQDDCBDSEFNQkVSUyBPRiBDT01NRVJDRSBST09UIC0gMjAxNjAc
Fw0xNjAyMTgxMDQyNDZaFw00MDAxMTMxMDQyNDZaMIHsMQswCQYDVQQGEwJFUzEPMA0GA1UEBwwG
TUFEUlklEMQ8wDQYDVQQIDAZNQURSSUQxQjBABgNVBAsMOXNlZSBpdCAyZW50IGFkZHJlc3MgYXQg
aHR0cHM6Ly93d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzczEiMCAGA1UECwwZQUMgQ0FNRVJGSVJN
QSBBQVBQlC0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRswGQYDVQQKDBJBQyBDQU1FUkZJUk1B
IFMuQS4xIjAgBgNVBAMMGUFDIENBTUVSRklSTUEgQUFQUCAtIDIwMTYwggIsMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQCwE4MTC6iG6bLAPM7HLIpdF+W0rPVWu7+bOnFYfcbkTruc+OPt12T
i1mhLGP8Ajm5lKLIXamDTb1ZAuCIgaoAjmU3PGpNm+ZxL3rMaPFhs79RVIyy0MezAwRbkJ8lbH6e
ajHtMxE1GH+MSqA1ONfT2mbpj+wK1T34sNdNKnxz5kN7MlNt2peQkyPVQ8p/mjO9omnfBgyFlaH
ot0HrAwNAat/hrvEyPtQ0EFDJhtpzbNAaFsY8eXoXOlNFo/Q1gFPgVORrF4kS3rHj6JzKp4tXpI4
43Ur/KW/0yGiag6HobFQ7sISq/631GPSosk0MmeKooHsi/3gr+IFHkQGFR863jxXLD7dKxyLzg7A
/x9tbiUIeGiFklm5ZU1Ai6+JqQaocMvAz/GOzm9aiXIuZkrwTo0rQ2+BYz/D+2wWrZ3+ehjHH0QP
7gU2DPvCA8NV7g4SzkAOZKv85gRqz1HD4b/KEmL9Mlg3/lbcfX5b0fhDP2KajBLue8i+GvnEgkl7
sp1nRaycHYGn3YvjIsf1ooSOj8ILb+R0XQ2Mt1uqH5V2DE34jB9ZR2s+cohWk5QIjfoSKuQWc4vV
3nNoI7JWQ9etHWkESGEW+TMR6GoMXkxEhfsxcd7VcyFOp6pDakdvdZ8b40d4o7xhrEDR9+wMRjF
MufipHWme9IlUn+5WiT+EQIDAQABo4IC8zCCAu8wEgYDVR0TAQH/BAgwBgEB/wIBAJAdBgNVHQ4E
FgQUjrZIBGcVDk+ZH8olMsiGITJRmh8wggEoBgNVHSMEggEfMIIBG4AUni5ITz5X9at9lsaL37M1
bUronouhgfikgfUwgfIxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1B
REJURDE6MDgGA1UECwwxc2VlIGN1cnJlbnQgYWRkcmVzczBhdCB3d3cuY2FtZXJmaXJtYS5jb20v
YWRkcmVzczEpMCcGA1UECwwgQ0hBTUJFUlMgT0YgQ09NTUVSQ0lgUk9PVCAtIDIwMTYxEjAQBgNV
BAUTCUE4Mjc0MzH4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSkwJwYDVQQDDCBDSEFN
QkVSUyBPRiBDT01NRVJDRSBST09UIC0gMjAxNoIINJojQbgJVDQwgYMGCCsGAQUFBwEBBHcwdTBL
BggrBgEFBQcwAoY/aHR0cDovL3d3dy5jYWllcmZpcm1hLmNvbS9jZX0cy9jaGFtYmVyc29mY29t
bWVyY2Vyb290LTIwMTYuY330MCYGCCsGAQUFBzABhhpodHRwOi8vb2NzcC5jYW1lcmZpcm1hLmNv
bTAOBgNVHQ8BAf8EBAMCAQYwJwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcD
ATA+BgNVHSAENzA1MDMGBFUdIAAwKzApBggrBgEFBQcCARYdaHR0cHM6Ly9wb2xpY3kuY2FtZXJm
aXJtYS5jb20wgY4GA1UdHwSBhjCBgzA/oD2gO4Y5aHR0cDovL2Nybc5jYW1lcmZpcm1hLmNvbS9j
aGFtYmVyc29mY29tWVyY2Vyb290LTIwMTYuY3JsMEGgPqA8hjpodHRwOi8vY3JsMS5jYW1lcmZp
cm1hLmNvbS9jaGFtYmVyc29mY29tbWVyY2Vyb290LTIwMTYuY3JsMA0GCSqGSIb3DQEBCwUAA4IC
AQCQlpeHxfz5ITiVMU6AQTBo7W7SQplRGvBfo4nzMVDFvpRC/4SXsXDj8iiqbk+5WyocPgT8f+t1
lzr9OApgWvv1CTkzma2bNHDeSk0wDTGfANJPXBjHozgXNC+TcA8XvI0AgM0UZRcYc85SW7V2GuX
sCKJtak4VmZBYcmzZXLC7g7KtWIUoIM0z1MgygU/8zSad+z9VEV/WfxOyXdu1WBsS/9JZ5N1M2
TZIqoq+iwXOBcEP1fi+lyC0SgDqX/8G8Jr9xLPx/HlkHTWy5LdeGyUwhu+As8NKroipYEDZGdHpN
0GubGTEOQjDYB4wXQ+7HBlqQfRnDUt7fQvLponnvYeR41hStQr8brhrzxfSyp1FSHtN3k4YYJQ/G
GyLrB0jgv/KzkHGwCTqn4wtu12W+3nKFmSUqIjcgSh+boxMuvDxUmLymHzHZQYyEjSH/LUQnftIK
o1RGqkaQ5tpj4XBdQ9uyzbjbX+onbcydy15d5NWjkwXopZkzYNzgHkqPaeMfUHmlc3BILJdwe8
8ANSXhS2tn4prZABmfmKGSMrOgdDNzcvrhpUeGeBHQ4qQKjDVKVRTQ4jCrBqcMAuW3sK/sdG/jw7
Ssesl30rCnFyR6Kt1ly8td3T58EvPj+hlr489FoFWXQUo+NlmPNLJCgp1TyVckWqEFF40nVljAmY5
7g==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA AAPP - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA AAPP - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Thu Feb 18 11:42:46 CET 2016*

Valid to: *Fri Jan 13 11:42:46 CET 2040*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B0:13:83:13:0B:A8:86:EA:12:C0:3C:CE:C7:2C:8A:5D:17:E5:B4:AC:F5:56:BB:BF:A1:FC:E9:C5:61:F7:9B:91:3A:6E:73:E3:8F:8B:5D:93:8B:59:A1:2C:63:FC:02:39:B9:94:A2:E5:C5:A9:83:4D:BD:59:02:E0:88:81:AA:00:8E:65:37:3C:6A:4D:9B:E6:71:2F:7A:CC:68:F1:61:B3:BF:51:56:5C:B2:D0:C7:B3:E3:04:5B:90:9F:25:6C:7E:9E:6A:31:ED:33:11:35:18:7F:8C:4A:A0:35:38:D7:D3:DA:66:E9:8F:EC:0A:D5:3D:F8:B0:D7:4D:2A:7C:73:E6:43:7B:32:53:6D:DA:97:90:93:23:D5:43:CA:7F:AE:68:CE:F6:89:A7:7C:18:32:16:56:87:A2:DD:07:AC:0C:0D:01:AB:7F:86:BB:C4:C8:FA:8E:10:50:C9:86:DA:73:6C:D0:1A:16:C6:3C:79:7A:17:38:83:45:A3:F4:35:80:53:EA:54:E4:6B:17:89:12:DE:B1:E3:EA:58:F3:2A:9E:2D:5E:92:38:E3:75:2B:FC:A5:BF:D3:21:86:6A:AE:87:A3:C1:50:EE:C7:D2:AB:FE:B7:D4:63:D2:A2:C9:34:32:67:8A:A2:81:EC:8B:FD:E0:AF:E2:45:1E:44:06:15:1F:3A:DE:3C:57:2C:3E:DD:2B:1C:8B:7A:0E:C0:FF:1F:6D:6E:25:08:78:68:85:92:59:B9:65:4D:40:8B:AF:89:A9:06:A8:70:CB:C0:CF:F1:8E:CE:6F:5A:89:72:2E:66:4A:F0:4E:8D:2B:43:6F:81:63:3F:C3:FB:6C:16:AD:9D:FE:7A:18:C7:1F:44:0F:EE:05:36:0C:FB:C2:03:C3:55:EE:0E:12:CE:40:0E:64:AB:FC:E6:04:6A:CF:51:C3:E1:BF:CA:12:62:FD:32:58:37:FD:F8:5C:7D:7E:5B:D1:F8:43:3F:62:9A:8C:12:EE:7B:C8:BE:1A:B9:C4:82:49:7B:B2:9D:67:45:AC:9C:1D:81:A7:DD:8B:E3:26:C7:F5:A2:84:8E:8F:C2:0B:6F:E4:74:5D:0D:8C:B7:5B:AA:1F:95:76:0D:FD:F8:8C:1F:59:47:6B:3E:72:88:56:93:94:08:8D:FA:12:2A:E4:16:73:8B:D5:DE:73:68:97:B2:56:43:D7:AD:E0:85:A4:11:21:84:5B:E4:CC:47:A1:A8:31:79:31:12:11:2C:89:E7:7B:55:EC:85:3A:9E:A9:0D:A9:1D:CB:86:7C:87:8D:1D:02:8E:F1:86:B1:03:47:DF:B0:31:18:C5:32:E7:EB:A4:75:A6:7B:D9:48:52:7F:B9:5A:24:FE:11:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *8E:B6:48:04:67:95:0E:4F:99:1F:CA:25:32:C8:86:21:32:51:9A:1F*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access

http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt

http://ocsp.camerfirma.com

Extended Key Usage *id_kp_clientAuth - id_kp_serverAuth*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://policy.camerfirma.com

CRL Distribution Points

http://crl.camerfirma.com/chambersofcommerceroot-2016.crl

http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B9:CC:D2:5E:63:36:48:F4:56:21:53:16:31:8B:6C:F4:52:C8:E0:76:DB:C6:F2:B1:32:1F:D8:39:2A:91:72:66*

X509SubjectName

Subject CN: *AC CAMERFIRMA AAPP - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA AAPP - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

	[es]	*undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

11.7.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

11.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.7.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA AAPP - 2016*

Subject O:	*AC CAMERFIRMA S.A.*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA AAPP - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject ST:	*MADRID*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*jrZIBGeVDk+ZH8olMsiGITJRmh8=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

11.7.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

11.7.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.7.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA AAPP - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA AAPP - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject ST:	*MADRID*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*jrZIBGeVDk+ZH8olMsiGITJRmh8=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2016-04-01T00:00:00Z*

11.7.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

11.8 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Camerales - 2016

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by the CA Camerfirma Camerales - 2016*

Name *[es]* *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5368777926801035574*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJcjCCB1qgAwIBAgISoG7FFTvETYwDQYJKoZIhvcNAQELBQAwgfIxCzAJBgNVBAYTAkVTMQ8w
DQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFIJRDE6MDgGA1UECwwxc2VlIGN1cnJlbnQgYWRk
cmVzcyBhdCB3d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzczEpMCcGA1UECwwgQ0hBTUJFUlMgT0Yg
Q09NTUVSQ0UgUk9PVCAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0Mzl4NzEbMBkGA1UECgwSQUMgQ0FN
RVJGSVJNQSBTLkEuMSkwJwYDVQQDDCBDSEFNQkVSUyBPRzBDT01NRVJDRSBST09UIC0gMjAxNjAe
Fw0xNjAyMTgxMTAyMTBaFw00MDAxMTMxMTAyMTBaMIIBEDELMAkGA1UEBhMCRVMxDzANBgNVBAgM
Bk1BRFJJRDEPMA0GA1UEBwwGTUFEUkIEMUIwQAYDVQQLDDIzZWUgY3VycmVudCBhZGRyZXNzIGF0
IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxNDAyBgNVBAsMK0FDIENBTUVSRkIS
TUEgQ0VSVEIGSUNBRE9TIENBTUVSQUxFUyAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0Mzl4NzEbMBkG
A1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMTQwMgYTVQQDDCUBQyBDQU1FUkZlUk1BIENFUlIRJRkID
QURPUyBDQU1FUkFMRVMgLSAyMDE2MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAt+KA
loYGS0/XIjg0gAN6TbXbRu2AHh4R3gB0/VgC+Nu6H0PVl7Qgjg2gU+LQfyN3lenZuqhmnSUhFH3p
3OsBGmFyiTyIWzHmpulhP3SiFPaoeZ5YGH9eUzm3LOu2CYlB1jZspMIxZ6qwtZWRG1kU4gYpb
8KemPJgEpF2K/JgCN/BdC80f9Q3n8bydVV4GzLtdutL8+HqOQ9QW7qw5uM6uwF1gt5vVm9uCUi5/lb
HcqPXfKyu48iuU0NH0aYMEcQaFrJ95S26BZIrZ3pHJDsY9Qo38BgeHeDeqUZ+OZ5E+ZPiO6xO7Tk
kFzGCBqorGXaj2nTpL2DRpn56kyRBxDte0RpmarytIKDj/WopK8yJU31kY7Ys02mdf5SiKRFFSEY
DNIHtCVhrohBFeikcQzfq/zLN9Ii8iMUBPs9g9nNPLHLIdoSlf37zmvNBaWTzYgRWStuSZMJ1uWc
dUWGHYbV/O7k7xnRtMDqgTLyRQVyv0+fcVbH2F4kqy290A5Bpz4G3XPBc4QKfbcvyMgk+IsDbumh
M3BAaMhWZstvKhEqdMEvGaQcDMmlPr5OdQu0LFKWC2y77a+vkJs4o0XQSM/+zqy3anBHYwZstFT
m1bru3h8zEtNKuS6Y9YJQuvPNAIvAgwmL61Q6SCy9+UwDufIUc9fvS8ujru+PJ7saFJLIwkCAwEA
AsOCAukwggLIMBIGA1UdEwEB/wQIMAYBAf8CAQIwHQYDVR0OBBYEFJeyWCR2bAmfGuSfrYpdzTT
hNTvMIIBKAYDVR0jBIIBHzCCARuAFJAuZU8+VWrZZbGr9+zNW1Ks6bLoYHdpHIMHyMQswCQYD
VQQGEwJFUzEPMA0GA1UECAwGTUFEUkIEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBj
dXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENJ
QU1CRVJTIE9GIENPTU1FUkNFIFJPT1QgLSAyMDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGzAZBgNV
BAoMEkFDMENBTUVSRkISTUEgUy5BLjEpMCcGA1UEAwwgQ0hBTUFUIMgT0YgQ09NTUVSQ0UgUk9P
VCAtIDIwMTaCCDSal0G4CVQ0MIGDBggrBgEFBQcBAQR3MHUwSwYIKwYBBQUHMAKGP2h0dHA6Ly93
d3cuY2FtZXJmaXJtYS5jb20vY2VydHMvY2hhbWJlcnNvZmNvbW1lcmNlcm9vdC0yMDE2LmNydDAm
BggrBgEFBQcwAYYaaHR0cDovL29jc3AuY2FtZXJmaXJtYS5jb20wDgYDVR0PAQH/BAQDAgEGMB0G
A1UdJQOWMBQGCCsGAQUFBwMEBggrBgEFBQcDAjA+BgNVHSAENzA1MDMGBFUdIAAwKzApBggrBgEF
BQcCARYdaHR0cHM6Ly9wb2spY3ku2FhZXJmaXJtYS5jb20wgY4GA1UdIwSBhjCBgzA/dD2gOMYS
aHR0cDovL2NybC5jYW1lcmZpcm1hLmNvbS9jaGFtYmVyc29mY29tbWVyY2Vyb2Vyb290LTIwMTYuY3Js
MECgPqA8hjpodHRwOi8vY3JsMS5jYW1lcmZpcm1hLmNvbS9jaGFtYmVyc29mY29tbWVyY2Vyb290
LTIwMTYuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQCMUlnDZGq0oGqcVnZcGM67WBCdCjMwNPUZv3v2
0vMVfBycH+8I3AYRQz3GmNGgt4koZyrmzyAb0BPP3YWXvL9Ze7dXQlLOd2G4MXXCihznnN3kw3uZ
A+4TiUlRgTZ58ytD9csVsgoti4pYiGTFZL3HKxfDN2FvgAgO99shwD4BxuEX87jmfCCaP+EZ8A
1ipehUuEMyHsWqdP+r1PKOZTcR7+Eah7G5drcouN3C6dkhU/60Dcn3lhKEPgm2dQTitUMZA8yQI3X
B76Z1mEdSLH4HxEwg1K4sGFfoxDqXNAhPpS/mIRBd/kEIIV4D4OnG86j5GdgsaGbaORd+7kL1Sn
T4gtvK13FPGzHUhJtbJ5SmBFbZ+wtrlLXzbubpMc3uGkzOJ6z3g7LQBiADV4tMRDTLCGKNmBO
a9PoCM90EqQY6ts6Z7KZk8VWN8TZSiiDRgDcbxa8nH4sXDXIOwIGSRabWPBlHv02ADpLeV8lKite
ygf5Jl5MeamUMcNmPWspimgcQHCmamMJZ5DkikFFS1gwNJtVD8W2vYiSZU3f6RjL5MTuerbpx2+n
z4gKzJml523U3oWhyM9OyBkDrf7cHx7vivHGMyiE77l/73lpOlw8clcGci04U9rrDxEpoP6Y63w
SSctxwDMRloCR33NpCjY720Ah8XopYNWwRLm+w==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L:	*MADRID*
Issuer ST:	*MADRID*
Issuer C:	*ES*
Subject CN:	*AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*
Valid from:	*Thu Feb 18 12:02:18 CET 2016*
Valid to:	*Fri Jan 13 12:02:18 CET 2040*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B7:E2:80:96:86:06:4B:4F:D7:22:38:34:80:03:7A:4D:B5:DB:46:ED:80:1E:1E:11:DE:00:74:FD:58:02:F8:DB:BA:1F:43:D5:97:B4:20:8E:0D:A0:53:E2:D0:7F:23:77:95:E9:D9:BA:A8:66:9D:25:21:14:7D:E9:DC:EB:01:1A:61:72:89:3C:A5:5A:2C:C8:1E:6A:6E:96:13:F7:4A:21:4F:6A:87:BF:67:96:06:1F:D7:94:CE:6D:CB:3A:ED:82:62:D0:75:8D:9B:29:30:8C:59:EA:AC:1F:65:64:46:D6:45:38:81:8A:5B:F0:A7:A6:3C:98:04:A4:5D:8A:FC:98:02:37:F0:5D:0B:CD:1F:F5:0D:E7:F1:BC:9D:55:5E:06:CD:47:6E:7C:BF:3E:1E:A3:90:F5:05:BB:AB:0E:6E:33:AB:B0:14:B8:25:E6:F5:66:F6:E0:94:E7:F9:5B:1D:CA:8F:5D:F2:B2:BB:8F:22:B9:4D:0D:1F:46:98:30:47:10:68:5A:C9:F7:94:B6:E8:16:48:AD:9D:E9:1C:90:EC:63:D4:28:DF:C0:60:78:77:83:7A:A5:19:F8:E6:79:13:E6:4F:88:EE:B1:3B:B4:E4:90:5C:C6:08:1A:A8:AC:65:DA:8F:69:D3:A4:BD:83:46:99:F9:EA:4C:91:07:10:ED:7B:44:69:99:AA:F2:B4:82:83:8F:F5:A8:A4:AF:32:25:4D:F5:91:8E:D8:B3:4D:A6:75:FE:52:88:A2:91:15:21:18:0C:D9:47:AC:25:61:AE:88:41:15:E8:A4:71:0C:DF:AB:FC:CB:37:D2:22:F2:23:14:04:FB:3D:83:D9:CD:3C:B1:CB:95:DA:12:95:FD:FB:CE:6B:CD:05:A5:93:CD:88:11:59:2B:6E:49:93:09:D6:E5:9C:75:45:86:1D:88:55:FC:EE:E4:EE:25:E7:F2:D3:03:AA:04:CB:C9:F4:15:CB:2D:3E:7D:C5:5B:1F:61:78:92:0C:B6:F7:40:39:06:96:78:19:73:C1:73:84:24:7D:B7:2F:C8:C8:24:FB:5B:03:6E:E9:A1:33:70:40:68:C8:56:66:CB:6F:2A:11:2A:74:C1:2F:19:A4:1C:0C:C9:88:3E:BE:4E:75:0B:B4:2C:52:96:0B:6C:BB:ED:AF:AF:90:9B:38:A3:45:D0:48:CF:FE:CE:AC:B7:6A:70:47:62:2C:19:B2:D1:53:9B:56:EB:BB:78:7C:CC:4B:4D:2A:E4:BA:63:D6:09:42:EB:CF:34:02:2F:02:0C:26:2F:AD:50:E9:20:AF:F7:E5:30:0E:E7:C8:51:CF:5F:BD:2F:2E:8E:BB:BE:3C:9E:EC:68:52:4B:23:09:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 2*
Subject Key Identifier	*97:A3:58:24:76:6C:09:9F:1A:E4:9F:AE:26:29:77:34:D3:84:D4:EF*
Authority Key Identifier	*9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*
Authority Info Access	*http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/chambersofcommerceroot-2016.crl* *http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *42:38:89:2F:E2:D3:34:A1:18:40:86:55:D6:9B:9F:A5:5D:81:A2:53:B1:28:D5:22:54:89:46:F9:DB:0A:F6:69*

X509SubjectName

Subject CN: *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-07-21T00:00:00Z

11.8.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

11.8.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.8.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by the CA Camerfirma Camerales - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*l6NYJHZsCZ8a5J+uJil3NNOE1O8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.8.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

11.8.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.8.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Camerales - 2016

Name [es] Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016

Service digital identities

X509SubjectName

Subject CN: AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

Subject O: AC CAMERFIRMA S.A.

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

Subject OU: see current address at https://www.camerfirma.com/address

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *l6NYJHZsCZ8a5J+uJil3NNOE1O8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-04-01T00:00:00Z*

11.8.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

11.9 - Service (withdrawn): Qualified Certificates issued by CA AC Racer-2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by CA AC Racer-2016*

Name *[es]* *Certificados Reconocidos emitidos por la CA Racer-2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *9748782597291380995*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJATCCBumgAwIBAgIJAIdKoh74EBEDMA0GCSqGSIb3DQEBCwUAMIHiMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUiklEMQ8wDQYDVQQHDAZNQURSSUQxQjBiBAtBgNVBAsMOXNlZSBjdXJvZW50IGFk
ZHJlc3MgYXQgaHR0cHM6Ly93d3cuY2FiZXJmaXJtYS5jb20vYWRkcmVzczEdMBsGA1UECwwUQUMg
Q0FNRVJGSVJNQSAtID1wMTYxEjAQBgNVBAUTCUE4Mjc0MzI4NzEbMBkGA1UECgwSQUMgQ0FNRVJG
SVJNQSBTLkEuMR0wGwYDVQQDDBRBQyBDQU1FUkZJUk1BIC0gMjAxNjAeFw0xNjAyMTgxNjEwMTha
Fw4zOTEyMTQxNjEwMThaMIHISMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFEUiklEMQ8wDQYDVQQH
DAZNQURSSUQxQjBiBAtBgNVBAsMOXNlZSBjdXJvZW50IGFkZHJlc3MgYXQgaHR0cHM6Ly93d3cuY2Fi
ZXJmaXJtYS5jb20vYWRkcmVzczEVMBMGA1UECwwMUkFDRVIgLSAyMDE2MRIwEAYDVQQFEwlBODI3
NDMyODcxGzAZBgNVBAoMEkFDIENB1TUVSRklST UEgUy5BLjEVMBMGA1UEAwwMUkFDRVIgLSAyMDE2
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEApIFB1TmYbpOHIzsTozGC8c3krMERx0o
/r5d8h5FiEWin+xosSnsiyiaY/5I3DQMk4QAUUlVqNQJne7S+kZKuP9wa98/6igSiCu6SUfztxij
Woz9J9lYat8onrrrldlNQwhe35oq3LVW+Sa705teoHNydTLjgjpLruqMUhZQVoxxTDduweP81UxR
0hRDsiSrnPX5VfXayYnoqwQWCyWUM39g6i/Wo173o39fHANTVE96bln9FhJcgR1NFz+Qe2EuJqn8
22ZeQ6kcU/WBM7Wd9FKfiZgucDx1Gg6b3SbSjZkhjMP0BP8HxpgbjnJkDqYxgrEF+cRWEvnA047An
cNK5b2ZOBzbjnJYIMQjC6In9sZzGkXy7YGi0NXSclpPIn1UfVbc44w9c4ldtVyVmkjPkPVDU
bkpmlqTMtONiPPp8gbF7tigU9N9QxX5gEOVcpXGWnVXNcptQOng/U7bxm6Yaz9XLfSSyep6+CpeC
Est1Oudg2ma72nS4+bfIAmv2zjTlbeNvuc3uujU0VZfDVX/TSSkLhkZ2yOWsq2zQjRldqu38z32
b0kVQ+p6EsWPreKccJBlmLRpWH1DZ/ljPJbWLE8KE8ukHXpsxVifGvbrC+zAEI5H6lZnQcZJ9BXn
HxAoxTLE6r6+t8RZWlrE8tmEWMjrvPT7GLU6zUUsmxBCAwEAAaOCAsYwggLCMBIGA1UdEwEBwQI
MAYBAf8CAQEwHQYDVR0OBBYEFLtxaMb7P6VjvAblCqpbOkZqYmhMMIIBJAYDVR0jBIIBGzCCARcA
FAgobscXAg3TTe/JonetWWgtXd9FoYH0pIHxMIHuMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFE
UklEMQ8wDQYDVQQHDAZNQURSSUQxQjA4BgNVBAsMMXNlZSBjdXJvZW50IGFkZHJlc3MgYXQgd3d3
LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxIzAlBgNVBAsMHkdMT0JBTCBDSEFNQkVSU0lHTiBST09l/
IC0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRswGQYDVQQKDBJBQyBDQU1FUkZJUk1BIFMuQS4x
JzAlBgNVBAMMHkdMT0JBTCBDSEFNQkVSU0lHTiBST09UIC0gMjAxNoIlcR0Sb0PwCgkwegY1KwYB
BQUHAQEEbjBsMEIGCCsGAQUFBzAChjZodHRwOi8vd3d3LmNhbWVyZmlybWEuY29tL2NlcnRzL2Fj
X2NhbWVyZmlybWEtMjAxNi5jcnQwJgYIKwYBBQUFMAGGGimhdtHA6L y9vY3NuLmNhbWVyZmlybWEu
Y29tMA4GA1UdDwEB/wQEAwIBBjAdBgNVHSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwPgYDVR0g
BDcwNTAzBgRVHSAAMCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vcG9saWN5LmNhbWVyZmlybWEuY29t
MHoGA1UdHwRzMHEwNqA0oDKGMGh0dHA6Ly9jcmwuY2FiZXJmaXJtYS5jb20vYWNlY2FiZXJmaXJt
YS0yMDE2LmNybDA3oDWgM4YxaHR0cDovL2NybDEuY2FiZXJmaXJtYS5jb20vYWNlY2FiZXJmaXJt
YS0yMDE2LmNybDANBgkqhkiG9w0BAQsFAAOCAgEAbGKruetlb6s8C4r0+dXkXBVYAeQZJsxlU67Y
IJTWIj3SA8U1jkRWIWZm+3lNyjogmuB+PgVrTXKDWXWft3X7ki+Ao3repUUfVbXTec5Ntg3G+vv+
awqoSRnMpJReAdPBqQIHt1gIrJAODKikENCoYqxKeqJXHDm/k/IVze1Cvna9EMFF0RMe1ZCi2Im
LOiXUcwM3ohss0aMmqnlKqGy1+BZfvxCgZzrpT5ZuDwgvJ+dBEU5V+ZoXSWCbbwLh3dIM87dA13B
AMpG2tQqCaCr/C3k43mG4UN7LYPbGGinufzSX0NOENNcbEIssB0R5ibQQCd N09Mk85TMd18Xowa0HH
bBH0duzZ4pYHdS1nVoqsL8o3OjlzriB9r3U7cjt/NV0r7l07eHuGUF0pYgtTocsWq2PVHVPt958
ZqLugp6Bz+OBgEKwWHTO9+uDXs+DnditbKMoit3AaEk7s8RvqVLVb3OERKqeOibRxSznkm4RDKCY
ZGcc3Rwnw3yQy2vr6x6/CCUVTfmsdhgBSMuCj8lCPDC7HUXOHiFkxKNjroOVUEgVPPyb7Ym2zk
YkzDfXmRL7dA/QztAYlbOQM4N8PHgypfkqVyTFGdhtYkH7j+rrk4RaNlmB1BJpcfXS7TAORFObc
6s16xFr+a66J8ZUdl88Nt1cvYa4JlQujRhd1cI=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *AC CAMERFIRMA - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *AC CAMERFIRMA - 2016*

Issuer OU: *see current address at https://www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *RACER - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU:	*RACER - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*
Valid from:	*Thu Feb 18 17:10:18 CET 2016*
Valid to:	*Wed Dec 14 17:10:18 CET 2039*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A4:81:41:D5:39:E7:61:BA:4E:1C:8C:EC:4E:8C:C6:0B:C7:B7:92:B3:04:47:1D:28:FE:BE:5D:F2:1E:45:88:45:9F:9F:EC:68:B1:29:EC:8B:28:9A:63:FE:48:DC:34:0C:93:84:00:51:49:55:A8:D4:09:9D:EE:D2:FA:46:4A:B8:FF:70:6B:DF:3F:EA:28:12:88:2B:BA:49:47:F3:B7:18:A3:5A:8C:FD:27:D9:58:6A:DF:28:9E:BA:EB:95:D9:4D:43:08:5E:DF:9A:2A:DC:B5:56:F9:26:BB:D3:9B:5E:A0:73:72:75:32:C9:82:3A:4B:AE:EA:8C:52:16:50:56:8C:71:4C:37:6E:C1:E3:FC:D5:4C:51:D2:14:43:B2:24:AB:9C:F5:F9:55:F5:DA:C9:89:E8:AB:04:16:0A:B5:94:33:7F:60:EA:2F:D6:A3:5E:F7:A3:7F:5F:1C:03:53:54:4F:7A:6E:59:FD:16:12:5C:81:1D:4D:17:3F:90:7B:61:2E:26:A9:FC:DB:66:5E:43:A7:5C:51:60:4C:ED:67:7D:14:A7:EB:66:0B:9C:0F:1D:46:83:A6:F7:4A:14:A3:66:48:63:30:FD:01:3F:C1:F1:A6:06:E3:9F:79:03:A9:8C:60:AC:41:7E:71:15:84:BE:70:34:E3:B0:27:70:D2:B9:6F:66:4E:07:36:FF:A6:22:58:21:F3:10:8C:2E:A5:9F:DB:23:65:E1:A4:5F:2E:D8:1B:43:63:5D:2A:C9:A4:F2:27:D5:47:D5:85:CE:38:C3:D7:38:D5:DB:62:57:25:66:92:33:E4:3D:50:D4:6E:4A:66:96:A4:CC:B4:E3:62:3C:FA:7C:81:B1:7B:B6:28:14:F4:DF:50:C5:7E:60:10:E5:5C:A5:71:96:9D:55:CD:72:9B:50:3A:78:3F:53:B6:F1:9B:A6:1A:CF:D5:CB:7D:24:B2:7A:9E:BE:0A:97:02:12:CB:75:3A:E7:60:DA:D9:DA:EF:69:D2:E3:E6:DF:7C:09:AF:DB:38:D3:95:B7:8D:BE:E7:37:BA:E8:D4:D1:56:5F:0D:55:FF:4D:24:A4:2E:19:19:DB:23:96:B2:AD:B3:42:34:65:76:AB:B7:F3:3D:F6:6F:49:15:43:EA:7A:12:C5:8F:AD:E2:9C:70:90:65:98:B4:69:58:7D:43:67:F9:63:3C:96:D6:2C:4F:0A:13:CB:A4:1D:7A:6C:C5:58:91:1A:F6:EB:0B:EC:C0:12:5E:47:E8:86:67:41:C6:49:F4:15:E7:1F:10:28:C4:52:C4:EA:BE:BE:8B:C4:59:5A:5A:C4:F2:D9:C4:58:C8:E2:BC:F2:3B:18:B5:3A:CD:45:2C:9F:1F:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 1*
Subject Key Identifier	*BB:71:68:C8:7B:3F:A5:63:BC:06:E5:0A:AA:5B:3A:46:6A:62:68:4C*
Authority Key Identifier	*08:28:6E:C7:17:02:0D:DF:4D:EF:C9:A2:77:AD:59:68:2D:5D:DF:45*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma-2016.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma-2016.crl* *http://crl1.camerfirma.com/ac_camerfirma-2016.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*A7:9D:0E:26:DB:A2:4A:A6:FC:B0:A4:7C:44:C7:CA:F6:F4:F5:DD:DE:F0:34:11:59:2D:4B:21:07:E1:0A:C7:2B*

X509SubjectName

Subject CN:	*RACER - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject SERIAL NUMBER:	*A82743287*

Subject OU: *RACER - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

11.9.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.9.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA AC Racer-2016*

Name *[es]* *Certificados Reconocidos emitidos por la CA Racer-2016*

Service digital identities

X509SubjectName

Subject CN: *RACER - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *RACER - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *u3FoyHs/pWO8BuUKqls6RmpiaEw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.9.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.9.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.9.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA AC Racer-2016*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA Racer-2016*

Service digital identities

X509SubjectName

Subject CN:	*RACER - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*RACER - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*u3FoyHs/pWO8BuUKqls6RmpiaEw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-04-01T00:00:00Z*

11.9.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.10 - Service (granted): Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Name *[es]* *Certificados Reconocidos emitidos por AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5859548927499719925*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJvjCCB6agAwIBAgIIUVFMtE+kVPUwDQYJKoZIhvcNAQELBQAwggEMMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBjdXlyZW50IGFk
ZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9G
IENPTU1FUkNFIFJPT1QgLSAyMDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVT
LUE4Mjc0MzI4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSkwJwYDVQQDCBDSEFNQkVS
UyBPRiBDT01NRVJDRSBST09tIlCIgzMjAxNjAeFw0xNjA0MTQwODQ4MDIaFw00MDAzMDkwODQ4MDIa
MIIBJDELMAkGA1UEBhMCRVMxDzANBgNVBAcMBk1BRFJlRDEPMA0GA1UECAwGTUFEUklEMUlwQAYD
VQQLDDlzZWUgY3VycmVudCBhZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2Fk
ZHJlc3MxMTAvBgNVBAsMKEFDIENBTUVSRkISTUEgRk9SIE5BVFVSQUwgUEVSL09OUyAtIDIwMTYx
EjAQBgNVBAUTCUE4Mjc0MzI4NzEYMBYGA1UEYQwPVkFURVMtQTgyNzQzMjg3MRswGQYDVQQKDBJB
QyBDQU1FUkZJUk1BIFMuQS4xMTAvBgNVBAMMKEFDIENBTUVSRkISTUEgRk9SIE5BVFVSQUwgUEVS
U09OUyAtIDIwMTYwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDScivlfis4NLgcRcki
77kcnZZAk5keFcjAtxYLCRsZRyTNe4nZAou7y6DudycjbXPhQveiGtYb9roXKs7KgatFuo8sk95
xyRdbtc6HDaP9HRIVHQAxCdXEdyWlvmlzSIK+QE1qPQtgrmYyhz3kyTpjBX18TUcMr3hLkMCx
x+jk2XQJRrbPI4OL39/Odfh10nWatyHdE4Tw70QgG2a5xOU1isvz4gHF3DnlqS0T0UCybZfBcQla
ojCBMwY1+GZtJvyTXAioxxwodc3dFZh109Q8TiMglz5YNxe9+Y1ytdt1voLCzB05yXp7ANRWFeZr
KvuI4PEqs1uKno63t7p0CalhwQqhIGQ0s9UJN9JPy5+y0rKIWTi7xcC2E1EEIK3b3oq+cJeMPXs
zHkPEJGO8IYQF8HIGqRTzFqr+fSqbl7HDTDD65/F4EsYgbkHwCX2ARyXCgMkBnv6J04VdKxZENf
IOMEe3gK39WR+cKJQOkEtHbeOLNyGQHDWL kmJFsPHHQ1fstPxL9Ug2Im/4zpNUm9lLXrg5amM0r
z7/GOk+tiXREqDEUrrYuhRtaYsu4eFbKPkdZ0s54btE9i3bHGyWqaZ7Ae6KhcLohzpp10zCvghYH
NCQYNdMS5zsBb+Tqcn5w7N0KJDesMJnCfR8xKzYWR94a5d0VkqY0YSw8GQIDAQABo4IDBjCCAwIw
EgYDVR0TAQH/BAgwBgEB/wIBAjAdBgNVHQ4EFgQUcLj4JMdRys4igJIlycBoL8FHWFEwggFFBgNV
HSMEggE8MIIBOIAUmSITz5X9at9kaL57M1bUrznouhggEUpIIBEDCCAQwxC2AJBgNVBAYTAkVT
MQ8wDQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFJlRDE6MDgGA1UECwwxc2VlIGN1cnJlbnQg
YWRkcmVzcyBhdCB3d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzczEpMCcGA1UECwwgQ00bBTUJFUlMg
T0YgQ09NTUVSQ0UgUk9PVCAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0MzI4NzEYMBYGA1UEYQwPVkFU
RVMtQTgyNzQzMjg3MRswGQYDVQQKDBIBQyBDQU1FUkZJUk1BIFMuQS4xKTAnBgNVBAMMIENlQU1C
RVJTIE9GIENPTU1FUkNFIFJPT1QgLSAyMDE2ggg0m2hggayszCBgwYIKwYBBQUHAQEEdzB1MEsG
CCsGAQUFBzAChj9odHRwOi8vd3d3LmNhbWVyZmlybWEuY29tL2NlcnRzL2NoYW1tZXJzb2Zjb21t
ZXJjZXJvb3QtMjAxNi5jcnQwJgYIKwYBBQUHMAGGGmh0dHA6Ly9vY3NwLmNhbWVyZmlybWEuY29t
MAAGA1UdDwEB/wQEAwIBBjAdBgNVHSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwPgYDVR0gBDcw
NTAzBgRVHSAAMCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vcG9saWN5LmNhbWVyZmlybWEuY29tMIGO
BgNVHR8EgYYwgYMwP6A9oDuGOWh0dHA6Ly9jcmwuY2FtZXJmaXJtYS5jb20vY2hhbWJlcnNvZmNv
bW1lcmNlcm9vdC0yMDE2LmNybDBAoD6gPIY6aHR0cDovL2NybDEuY2FtZXJmaXJtYS5jb20vY2hh
bWJlcnNvZmNvbW1lcmNlcm9vdC0yMDE2LmNybDANBgkqhkiG9w0BAQsFAAOCAgEAlegXSJ31a4pj
k3tS5X9kkee6+HoEARQGrtrTs/k/1+DyDe7jrjMvxt1fI5EhL3zU0lG//L1dgTnOZjv5CpgzVxXV
Kq2R4ezrSCvR2j4MWOdF/ylbLn011t3MSRVv1smk56zOy+jjlkT/pvQ4SLdOqpbLkY0sL0Jk1fg
ZQ6yPo1U+gvPVoyYvdJC2tPFlx2sw9Kb5LAPSwC7robREdGX9J5VjAJSjGf7ZfPZ3Q77OcBTUsi2
ypcHmANGEtBL5FUadhVkzYWz7C3pRgGr7y97/oL z+NaSU6TdgsHLC3HxTSz7IEIqV8DTmIC3zt
5jFW4fcfMOuRlLbDTpPVhJjAJSVhubbxAN8id45OLEb8lafuEhaGHL1DFavXbrV+d1ich4H3kfh4
lEd7gMUX5jkT+rTCokaxdXfzQOS8gTuGuHnUoV6oay3lqRTYo/hpKJdU3PoY8JE9CeDcTxtmVSph
M6cFMYZmAqVNccZWa0+4YfF8cqL/KcEW2pIJSQwSz+dayEukwW0VTGeIuXuzO068/JMHTr8zkia
syvE+jJ8T+Zr82YXMqENEZ/MBrbB34Tm7YGMSxVq3/kwIW7AfoxOJEXsnlZUsRMlP8vDS1yrGx/8
9vJ7q06cAXjZ2msn+BnV8JxBNo8BhHtM/Nwk1aBsI8MkknGMpz09+JbCICDK4xU=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject ST:	*MADRID*
Subject L:	*MADRID*
Subject C:	*ES*
Valid from:	*Thu Apr 14 10:48:09 CEST 2016*
Valid to:	*Fri Mar 09 09:48:09 CET 2040*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:72:2B:E5:7E:DB:38:34:B8:1C:45:C9:22:EF:B9:1C:9D:9D:80:93:99:1E:15:C8:C0:B7:16:0B:09:1B:19:47:24:CD:7B:89:D9:02:8B:BB:CB:A0:EE:77:27:23:6D:73:E1:42:F7:A2:1A:D6:1B:FF:DA:E8:5C:AB:3B:2A:06:AD:16:EA:3C:B2:4F:79:C7:24:5D:89:BB:5E:6C:70:DA:3F:D1:D1:95:51:D0:03:10:9D:5C:47:72:5A:5B:E6:23:34:88:2B:E4:04:D6:A3:D0:B6:AC:A6:FF:26:32:86:2D:E4:C9:3A:63:05:7D:7C:4D:47:8C:AF:78:4B:90:C0:B1:C7:E8:E4:D9:74:09:46:B6:CF:23:83:8B:DF:DF:CE:75:F8:75:D2:75:9A:B7:21:DD:13:84:F0:EF:44:20:1B:66:B9:C4:E5:35:8A:CB:F3:E2:01:C5:DC:39:C8:A9:2D:13:D1:40:B2:6D:97:C1:71:09:5A:A2:30:81:33:06:08:F8:66:62:26:FC:93:5C:08:A8:C7:1C:28:75:CD:DD:15:98:75:D3:D4:3C:4E:D3:20:97:3E:58:37:17:BD:F9:8D:72:B5:DB:75:BE:82:C2:CC:1D:39:C9:7A:7B:00:D4:56:15:E6:6B:2A:FB:A5:8B:83:C4:AA:CD:6E:46:7A:3A:DE:DE:E9:D0:26:88:87:04:2A:84:81:90:D2:CF:54:24:DF:49:3F:2E:7E:CB:4A:CA:95:64:E2:EF:17:02:D8:4D:44:12:52:B7:6F:7A:2A:F9:C2:5E:30:F5:EC:CC:79:0F:10:93:8E:F2:56:10:17:C1:C8:1A:A4:53:78:5A:BE:F9:FE:6A:0C:8E:C7:0D:30:C3:EB:9F:C5:E0:4B:18:81:B9:07:C0:25:F6:03:F4:72:5C:28:0C:29:B8:6F:E8:9D:38:57:82:AF:64:43:5F:20:E3:04:7B:78:0A:DF:D5:91:F9:C2:89:40:E9:04:88:78:5E:38:B3:72:19:01:C3:58:B9:26:24:5B:0F:1C:74:35:7E:CB:4F:C4:BF:54:83:62:66:FE:2E:33:A4:D5:26:F6:52:D7:AE:0E:5A:98:CD:2B:CF:BF:C6:3A:4F:A2:7D:74:44:A8:31:14:AE:B6:2E:85:18:DA:62:CB:B8:78:56:CA:3E:47:59:D2:CE:78:6E:D1:3D:8B:76:C7:1B:25:AA:69:9E:C0:7B:A2:A1:70:BA:21:CE:9A:75:D3:30:AF:82:16:07:34:24:18:35:D3:12:E7:3B:01:6F:E4:EA:72:7E:70:EC:DD:0A:24:37:AC:30:99:C2:7D:1F:31:2B:36:16:47:DE:1A:E5:DD:15:92:A6:34:61:2C:3C:19:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 2*
Subject Key Identifier	*70:B8:F8:24:C7:51:CA:CE:22:80:92:08:C9:C0:68:2F:C1:47:58:51*
Authority Key Identifier	*9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*
Authority Info Access	*http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/chambersofcommerceroot-2016.crl* *http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*EE:DD:45:7A:F1:35:3D:76:F4:8E:7C:61:23:F3:91:40:E5:F9:A0:69:CA:51:B4:3E:EA:86:15:C9:CE:C0:D4:BB*

X509SubjectName

Subject CN:	*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*

Subject OU: *AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

11.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.10.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.99.18.1*

Description

11.10.3 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Name *[es]* *Certificados Reconocidos emitidos por AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject ST:	*MADRID*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*cLj4JMdRys4igJIIycBoL8FHWFE=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2016-06-23T22:00:00Z*

11.11 - Service (granted): Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Service digital identities

Certificate fields details

Version:	*3*

Serial Number: *6102780882998024770*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIUojCCB6KgAwIBAgIIVLFu4REkWkIwDQYJKoZIhvcNAQELBQAwggEMMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFk
ZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9G
IENPTU1FUkNFIFJPT1Qgl.SAyMDE2MRIwEAYDVQQFEwIBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVT
LUE4Mjc0MzHNzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMS4wJwYDVQQDCBDSEFNQkVS
UyBPRiBDT01NRVJDRSBST09UIC0gMjAxNjAeFw0xNjA0MTQwODMzMDdaFw00MDAzMDkwODMzMDda
MIIBIDELMAkGA1UEBhMCRVMxDzANBgNVBAcMBk1BRFJlRDEPMA0GA1UECAwGTUFEUklEMUlwQAYD
VQQLDDlzZWUgY3VycmVudCBhZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2Fk
ZHJlc3MxLzAtBgNVBAsMJkFDIENBTUVSRkISTUEgRk9SIExFR0FMIFBFUlNPTlMgLSAyMDE2MRIw
EAYDVQQFEwIBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVTLUE4Mjc0MzHNzEbMBkGA1UECgwSQUMg
Q0FNRVJGSVJNQSBTLkEuMS8wLQYDVQQDDCZBQyBDQU1FUkZJUk1BIEZPUiBMRUdBTCBQRVJTT05T
IC0gMjAxNjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAM5b139kUoBuAH5mGwLI2KA3
6vuD+cIMc7HzzFT8SGehGE6PloNM0hrSh/Xhf+oi6eoyzkGtaAmaGYZmlbW//pxjd6x7DHZyquf
qtD49aPsEwL6pNKecFb5bJdMBQ2D2pSmxPjNYoAcesw8hzhTgzNzg+jWvtcL/H5Bv9czVFRKZOA
zuSNCqnz3djGW04BBBVoZN19btuPaQdfghlyKTGCjycXoL4I5NRZEUm+KbuEYdfya2Q4o0iLbmtx
ZHXd+4+5FZ3ww4O0A07K1FNylZHoSRPYuSdE97dlXJMq9L2uzcQPqk1KJOrxELTsT0XZXe0epnwQ
cleVTV4pf33a9cuXc7HRjUGwa5MthTWEUhSBg+IQeaMegVoyxAISLSRWh+oI5GKEA5XyeVM5gI25
VbtbWV9yX3NdlEBkknNwVx4IVBfphvBuSM6fpS/sS7IttHv58zBhSA7aclxzTzKV9ts1SsN2gGFNP
Yv8lAcWgNbn2ppqRBU3EDzJM+xm0Gsjo/Vz2KIoiRoGHZR8v0ySx+BKgloTdU2/uEwBTKM0xk7ge
vax8IGagdpKn2bOnAK8suw36V695tUQsPGKUceXQTwQUZaxTHiqynlYZVXG3kLNYrKC0ZuGrDZt
huYU2pEsQWxLQkTyPa0fAjkoAbA1LU4rgkWunrUgGkVVdABxtZoXAgMBAAGjggMGMIIDAjASBgNV
HRMBAf8ECDAGAQH/AgECMB0GA1UdDgQWBBTD4WT1y+WxRusdPZhqJKfWgUQjCCAiUGA1UdIwSC
ATwwggE4gBSeLmVPPlf1ta32WxovfszVtSuce6GCARSkggEQMIIBDDELMAkGA1UEBhMCRVMxDzAN
BgNVBAgMBk1BRFJlRDEPMA0GA1UEBwwGTUFEUklEMTowOAYDVQQLDDFzZWUgY3VycmVudCBhZGRy
ZXNzIGF0IHd3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzMSkwJwYDVQQLDCBDSEFNQkVSUyBPRiBD
T01NRVJDRSBST09UIC0gMjAxNjESMBAGA1UEBRMJOTgyNzQzMjg3MRgwFgYDVQRhDA9lVQVRFUv1B
ODI5NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkISTUEgUy5BLjEpMCcGA1UEAwwgQ0hBTUFUlMg
T0YgQ09NTUVSQ0UgUk9PVCAtIDIwMTaCCDSaLaGCBrKzMIGDBggrBgEFBQcBAQR3MHUwSwYIKwYB
BQUHMAKGP2h0dHA6Ly93d3cuY2FlZXJmaXJtYS5jb20vY2VydHMvY2hhbWJlcnNvZmNvbW1lcmNl
cm9vdC0yMDE2LmNydDAmBggrBgEFBQcwAYYaaHR0cDovL2ljc3AuY2FlZXJmaXJtYS5jb20wDgYD
VR0PAQH/BAQDAgEGMB0GA1UdQQWMBQGCCsGAQUFBwMEBggrBgEFBQcDAjA+BgNVHSAENzA1MDMG
BFUdIAAwKzApBggrBgEFBQcCARYdaHR0cHM6Ly9wb2xpY3kuY2FlZXJmaXJtYS5jb20wgY4GA1Ud
HwSBhjCBgzA/oD2gO4Y5aHR0cDovL2NybC5jYW1lcmZpcm1hLmNvbS9jaGFtYmVyc29mY29tbWVy
Y2Vyb290LT1wMTYuY33sMECgPqA8hjpodHRwOi8vY3JsMS5jYW1lcmZpcm1hLmNvbS9jaGFtYmVy
c29mY29tbWVyY2Vyb290LTIwMTYuY33sMA0GCSqGSIb3DQEBCwUAAAICAQAVmhmr8Ye5zwqQbUIi
TgPJ7QTf8yQUAkwHtFXSed6LhCwyT1Xj4FK4YD3lW3l98cRfeHUWvatFv/3YXN3+kog/76f9aEKA
UwwUCSBte0ArzAxLKb+SzZvO6JE+fQIK44VRSLIVz6zq+ueM95P6F4f0elRpMYHGHLM1aN7dYKLs
7mMs8Da6DGXBpRy1mBU2L4u8iMcRjM4PJmUXvfOsU9ETQjLv5Kjym1LwiQ2ytsJuT5pTD7HSmdh
a/73kBSqOGmu6iLC7pooiHz85o1reFbZM1VdvqVfqac/Rpu6hw7mzZAqQSZ0b+DhzgYXiQ7wT1
L03jYlrQQMry2rlHA3te3YYKayi4vHmVk6d0SmMw3VHoVAFBtRM24Gg3XsqxnCqbCoNuNOSg85E5
5Dcgxsw9MCntnxUJ0wDNHcl7Pv1zTqkLlshfYXOdQFVcoE+o2d/9PZ/GthfwtSm1hrRSN7lyXBOP
zptm1RdWJeXbzxD4kGPmDE3+pSX617vi+lrx3pU8x1itdP75byfcSrd0XJcDNfr2LYfXYV4bKwg
Nc4zTbKc+9SDyfrohtaDkYjUZFoldqmMU/TCAcZtiM95AOiV6mfEWfdyXqYmi5Mh3deWsI7oUgiS
22bcOgdnklAHfxkpFHGUACljZqGbxBelhX0rYJwAPmPU8rpGV1Bn4CxHw==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L:	*MADRID*
Subject C:	*ES*
Valid from:	*Thu Apr 14 10:33:07 CEST 2016*
Valid to:	*Fri Mar 09 09:33:07 CET 2040*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CE:5B:D7:7F:64:52:80:6E:00:7E:66:1B:02:C8:D8:A0:37:EA:FB:83:F9:C2:0C:73:B1:F3:CC:54:FC:E4:67:A1:18:4E:8F:22:83:4C:D2:1A:D2:87:F5:E1:17:EA:22:D1:EA:32:CE:41:AD:68:0B:67:68:66:19:9A:56:D6:FF:FA:71:8D:DE:B1:EC:31:D9:CA:AB:89:A9:F0:F8:F5:A3:EC:13:02:DF:7A:95:9E:78:56:D2:6C:9E:2D:30:14:36:97:6A:52:9B:13:E3:35:8A:00:79:EB:30:F2:17:21:4E:06:4D:CE:0F:A3:5A:FD:1C:2F:F1:F9:06:FF:5C:CD:51:51:29:93:80:CE:E4:8D:0A:A9:F3:DD:D8:C6:5B:4E:01:04:15:68:64:DD:7D:6E:DB:8F:69:07:5F:82:19:72:29:31:82:8F:27:17:A0:BE:08:E4:D4:59:11:49:BE:29:BB:84:61:D7:F2:6B:64:38:A3:48:8B:6E:6B:71:64:75:DD:FB:8F:B9:15:9D:F0:C3:83:B4:03:4E:CA:D4:53:72:21:91:E8:49:13:D8:B9:27:44:F7:B7:49:5C:93:2A:F4:BD:AE:CD:C4:0E:AA:4D:4A:24:EA:F1:10:B4:EC:4F:45:D9:5D:ED:1E:A6:7C:10:7A:57:95:4D:5E:29:7F:7D:DA:F5:CB:97:73:B1:D1:8D:41:B0:6B:93:2D:85:35:84:52:14:81:83:E2:10:79:A3:1E:81:5A:32:C4:09:52:2D:24:56:87:EA:1F:E4:62:84:03:95:F2:79:53:39:80:8D:B9:56:1B:61:59:5F:6F:5F:73:5D:94:40:64:92:73:70:57:1E:08:54:17:E9:86:F0:6E:48:CE:88:A7:9F:EC:4B:B0:ED:1E:FE:7C:CC:18:52:03:B6:9C:23:1C:D3:CC:A5:7D:B2:F2:39:B0:DD:A0:18:53:4F:62:FF:25:01:C5:A0:35:B9:F6:A6:9A:91:05:4D:C4:0E:B2:4C:FB:19:B4:1A:C8:E8:FD:5C:F6:28:8A:22:46:81:87:65:1F:2F:D3:24:B1:F8:12:A0:96:84:DD:53:6F:EE:13:00:53:28:CD:31:93:B8:1E:BD:AC:7C:10:81:9A:81:DA:4A:9F:66:CE:9C:02:BC:B2:EC:37:E9:5E:BD:E6:D5:10:B0:F1:8A:51:E7:97:41:3C:10:51:96:B1:4C:78:AA:CA:79:58:65:55:C6:DE:42:CD:62:B2:82:D1:9B:86:AC:36:6D:86:E6:14:DA:91:22:41:6C:4B:42:44:F2:3D:AD:1F:02:39:28:01:B0:35:2D:4E:2B:82:45:AE:9E:B5:2A:1A:45:55:74:00:71:B5:9A:17:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 2*
Subject Key Identifier	*C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*
Authority Key Identifier	*9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*
Authority Info Access	*http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/chambersofcommerceroot-2016.crl* *http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*3A:80:66:26:6D:28:BD:28:CC:D0:F5:64:C8:FB:C1:21:9B:4F:FA:E4:03:E0:1E:50:39:D3:0F:24:00:F0:EB:09*

X509SubjectName

Subject CN:	*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-03-15T01:00:00Z*

11.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

11.11.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.99.18.1*

Description

11.11.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Name *[es]* *Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject ST:	*MADRID*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*wyeFk9cvlsUbrHYz2YaiSn1oFEI=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2017-07-21T00:00:00Z*

11.11.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.11.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

11.11.4 - History instance n.2 - Status: granted

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject ST:	*MADRID*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*wyeFk9cvlsUbrHYz2YaiSn1oFEI=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

11.11.4.3 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2*

11.11.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.11.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject ST:	*MADRID*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*wyeFk9cvlsUbrHYz2YaiSn1oFEI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-23T22:00:00Z*

11.11.5.5 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2*

11.12 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1227365184625606914*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJmDCCB4CgAwIBAgIIEQb6le9KgQIwDQYJKoZIhvcNAQELBQAwgfwxCzAJBgNVBAYTAkVTMQ8w
DQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFJJRDFCMEAGA1UECww5c2VIIGN1cnJlbnQgYWRk
cmVzcyBhdCBodHRwczovL3d3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzMR0wGwYDVQQLDBRBQyBD
QU1FUkZJUk1BIC0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3
NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkJSTUEgUy5BLjEdMBsGA1UEAwwUQUMgQ0FNRVJGSVJN
QSAtIDIwMTYwHhcNMTYwNDE0MTUxMzM0WhcNNDAwMjA4MTUxMzM0WjCCATIxCzAJBgNVBAYTAkVT
MQ8wDQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFJJRDFCMEAGA1UECww5c2VIIGN1cnJlbnQg
YWRkcmVzcyBhdCBodHRwczovL3d3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzMTgwNg YDVQQLDC9B
OyBIQU1FUkZJUk1BIEdMT0JBTCBGT1IgTk1UVVJBTCBQRVJTT05TIC0gMjAxNjESMBAGA1UEBRMJ
QTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRklS
TUEgUy5BLjE4MDYGA1UEAwwvQUMgQ0FNRVJGSVJNQSBHTE9CQUwgRk9SIE5BVFVSQUwgUEVSU09O
UyAtIDIwMTYwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCrM224Vese/k6tN9vlyIfx
eG72kworDpNMywaVwyb6mgolSsKzrlvCO/EwbRtsVB4Uhq61Bxm9ebnOyrlj12ozw19goqd2lqPb
chRD0uy1ZEtrpozo4n2Rz/RpuGQfHdlCkUs3Ps84VDcyANtrHMfQfJdTzqT2++aHgEftIZAtXRBV
SjUdFtPkDsInGrzYfiny/bA765MsLFhkHO5tpbqvb6w/OG4zalavZunG7lFgRgrV/t6Z38T9xsTi
3fUASxQ5vpi76cuRkzGZZ440Lvbeek NDMHWb5uCrZZgBF440pEPiTW4gJra+FsnPSLBEmXIU3vV
z5CBubTunGmMKZjonSOOnW56PaGzd92J+s1jzx65OET+lXXnhOolUch1k5q5pvrut2gtka+VNwfAk
SiRWOSIQOcW2gzSQTCjF7dNNOi0iDZQ13B6A9EamGbdtbXkAdYugnd5caVUSbdZ1hP9Wp9uIbcht
uhLAwQYhcOA66lFwKQcdnsUEJYiC8bYntNwfjIxD8aNUzR2i4gfURJpoYB97NVEMZjq+keSdLNaL
0hwirjqnsA6GORxcvTqCzduCm05HE8CkFM/tgucL69151f7sJmO1my6PsBNCOQdTnbdIEBk87WtY
5wFk6qFLp7+zyTI9+1bWGT/WRt7GZR8TWRvcuQhbuJMcp9TdWTv2jQIDAQABo4IC4zCCAtswEgYD
VR0TAQH/BAgwBgEB wIBATAdBgNVHQ4EFgQUTjZWgFiOG4OFYEzUG6Hfcj2ve18wggFBBgNVHSME
ggE4MIIBNIAU0oSXRE3ZjO58Jb95gLMpSJuLGlShggEOpIfBDDCCAQgxCzAJBgNVBAYTAkVTMQ8w
DQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFJJRDE6MDgGA1UECwwxc2VIIGN1cnJlbnQgYWRk
cmVzcyBhdCB3d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzczEnMCUGA1UECwweR0xPQkFMIENIQU1C
RVJTSUdOIFJTT1QgLSAyMDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVTLUE4
MjcOMzI4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMScwJQYDVQQDDB5HTE9CQUwgQ0hB
TUJFUlNJR04gUk9PVCAtIDIwMTaCCBEIcVpXS6RNMHoGCCsGAQUFBwEBBG4wbDBCBggrBgEFBQcw
AoY2aHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9hYI9YW1lcmZpcm1hL1IwMTYuY3J0
MCYGCCsGAQUFBzABhhpodHRwOi8vb2NzcC5jYW1lcmZpcm1hLmNvbTAOBgNVHQ8BAf8EBAMCAQYw
HQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMDMGA1UdIAQ3MDUwMwYEVR0gADArMCkGCCsG
AQUFBwIBFh1odHRwczovL3BvbGljeS5jYW1lcmZpcm1hLmNvbTB6BgNVHR8EczBxMDagNKAyhjBo
dHRwOi8vY3JsLmNhbWVyZmlybWEuY29tL2FjX2NhbWVyZmlybWEtMjAxNi5jcmwwN6A1oDOGMWh0
dHA6Ly9jcmwxLmNhbWVyZmlybWEuY29tL2FjX2NhbWVyZmlybWEtMjAxNi5jcmwwDQYJKoZIhvcN
AQELBQADggIBALsqO9QPJPA2fbM+E0z3ZZc0hz0vzuar9vEhq9JMs4BPKkwqvSmc0IU90Dz+rLYZAS+
3w87olqKd98f2MnjYjHi40siDGL3DtzoDorucF9uiPqf5q29wnib6kSp49vnYXNbYDeS+uyE0UVK
V7VbnEPdX6/BDfbBcpLaga0OkS/D4TMF11btv0QBhMZSIndyHF37yuTHWS8ILMcgattemn4ypRoD
ObJDIf6wpcTaAzijdqaBLXQ37hsfivhF3DzWGLFFzW1ls0O6KQjb7mfNS191NV4lF8XIskie6PX7
Y6EUlagUbqgHkcJ3mqfXVxjbqKEShy6cfFKMpnX7F7ONoTielyBCXQVnCENwu9E4OtrEhee
Hk+nZ603kSj0TizmGWejXKahdUlWuT/BgM5p7mBcK74wfuYsXbwXBOKKU+fmRnwGmiQvM80ld+fj
1vXo3AaYcqM6fRWsv9fWpNgcRIHUMF9rh1H/wwvhuRLLYUMFMjYbdlpV32oPosoVEdhdSZdq2LLp
aWjy68Pg+I5C7CkdZ+LEjl/q8bm4+4NYIXxU/wEowRWQT+rJ4txA8w4wvPrDhIYbDdPNRB/VzdkJD
RgNRHHNHjtIlpXjL5ZiKqawhaCESfoBTPmfK+96IYMtDup38kmnV0FB7Horuz7t0INa09Kwm5dK7
bcrftuUkdz+L

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC CAMERFIRMA - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *AC CAMERFIRMA - 2016*

Issuer OU: *see current address at https://www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST:	*MADRID*
Subject C:	*ES*
Valid from:	*Thu Apr 14 17:13:34 CEST 2016*
Valid to:	*Wed Feb 08 16:13:34 CET 2040*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AB:33:6D:B8:55:EB:1E:FE:4E:AD:37:DB:E5:C8:87:F1:78:6E:F6:93:0A:2B:0E:93:4C:CB:06:95:C3:26:FA:9A:0A:08:4A:C2:B3:AE:5B:C2:3B:F1:30:6D:1B:6C:54:1E:14:86:AE:B5:07:19:BD:79:B9:CE:CA:B9:63:D7:6A:33:C3:5F:60:A2:A7:76:96:A3:DB:72:14:43:D2:EC:B5:64:4B:6B:A6:8C:EE:E2:7D:91:CF:F4:69:B8:64:1F:1D:D2:C2:91:4B:37:3E:8F:38:54:37:32:00:DB:6B:1C:C7:D0:95:37:53:CE:A4:F6:FB:E6:87:80:41:6D:21:90:2D:5D:10:55:4A:35:1D:16:D3:E4:0E:C2:27:1A:BC:D8:7E:29:F2:FD:B0:13:EB:93:2C:2C:58:64:1C:EE:6D:A5:BA:AF:6F:AC:3F:38:6E:33:6A:56:AF:66:E9:C6:EE:51:60:46:0A:D5:FE:DE:99:DF:C4:FD:C6:C4:E2:DD:F5:00:4B:14:39:BE:98:BB:E9:CB:91:93:31:99:67:8E:34:2E:F6:DE:7A:43:43:30:75:9B:E6:ED:AD:FD:96:60:04:5E:38:D2:91:0F:89:35:B8:80:9A:DA:F8:5B:27:3D:22:C1:12:65:C8:53:CB:D5:CF:90:81:B9:B4:EE:9C:69:8C:29:98:E8:9D:23:8E:9D:6E:7A:3D:A1:B3:77:DD:89:FA:CD:62:CF:1E:B9:38:44:FE:95:75:E7:84:EA:14:72:1D:64:E6:AE:69:BE:BB:AD:DA:07:E4:6B:E5:4D:C1:F0:24:4A:24:56:39:22:50:39:C5:B6:82:BE:50:4C:28:C5:ED:D3:4D:3A:2D:3F:65:0D:77:07:A0:3D:11:A9:86:6D:DA:DB:5E:40:1D:B5:8B:A0:9F:F7:52:71:A5:54:49:B7:73:D6:13:FD:5A:9F:5A:0D:C8:6D:BA:12:C0:C1:06:21:70:E0:3A:EA:51:70:29:07:9D:9E:C5:04:25:88:82:F1:B6:27:7C:DC:1F:8E:5C:43:F1:A3:54:CD:1D:A2:E2:07:D4:44:8A:68:60:1F:7B:35:51:0C:66:3A:BE:91:E4:9D:2C:D6:8B:D2:1C:22:AE:3A:A7:B0:0E:86:39:1C:5C:BD:3A:82:CD:DB:82:9B:4E:47:13:C0:A4:14:CF:ED:82:E7:0B:EB:DD:79:7C:5E:EC:26:63:B5:9B:2E:8F:B0:13:42:39:07:53:9D:B7:65:10:19:3C:ED:6B:58:E7:01:64:EA:A1:4B:A7:BF:B3:C9:32:3D:FB:56:D6:19:3F:D6:46:DE:C6:65:1F:13:59:1B:DC:B9:08:5B:B8:93:1C:A7:D4:DD:59:3B:F6:8D:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 1*
Subject Key Identifier	*4E:36:56:A8:58:CE:1B:83:85:60:4C:D4:1B:A1:DF:72:3D:AF:7B:5F*
Authority Key Identifier	*D2:84:97:44:4D:D9:88:EE:7C:25:BF:52:80:B3:29:48:9B:8B:18:84*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma-2016.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma-2016.crl* *http://crl1.camerfirma.com/ac_camerfirma-2016.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*EF:41:1C:83:7A:C3:30:41:85:E5:39:13:FE:36:9B:F8:FF:65:98:C2:A5:2B:DB:1B:6E:2D:EA:B5:DC:C7:F0:6F*

X509SubjectName

Subject CN:	*AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*

Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

11.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.12.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *TjZWqFjOG4OFYEzUG6Hfcj2ve18=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.12.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.12.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Name *[es]* *Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *TjZWqFjOG4OFYEzUG6Hfcj2ve18=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-23T22:00:00Z*

11.13 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Name *[es]* *Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3785224270412042658*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJlDCCB3ygAwIBAgIlNIfRa0EY0aIwDQYJKoZIhvcNAQELBQAwgfwxCzAJBgNVBAYTAkVTMQ8w
DQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFJJRDFCMEAGA1UECww5c2VlIGN1cnJlbnQgYWRk
cmVzcyBhdCBodHRwczovL3d3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzMR0wGwYDVQQLDBRBQyBD
QU1FUkZJUk1BIC0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3
NDMyODcxGzAZBgNVBAoMEkFDIENB1TUVSRkISTUEgUy5BLjEdMBsGA1UEAwwUQUMgQ0FNRVJGSVJN
QSAtIDIwMTYwIHlcNMTYwNDE0MTQ1ODM2WhcNNDAwMjA4MTQ1ODM2WjCCAS4xCzAJBgNVBAYTAkVT
MQ8wDQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFJJRDFCMEAGA1UECww5c2VlIGN1cnJlbnQg
YWRkcmVzcyBhdCBodHRwczovL3d3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzMTYwNAYDVQQLDC1B
QyBDQU1FUkZJUk1BIEdMT0JBTCBGT1lgTEVHQUwgUEVSU09OUyAtIDIwMTYxEjAQBgNVBAUTCUE4
Mjc0MzI4NzEYMBYGA1UEYQoPVkFURVMtQTgyNzQzMjg3MRowGQYDVQQKDBIBQyBDQU1FUkZJUk1B
IFMuQS4xNjA0BgNVBAMMLUFDIENBTUVSRkISTUEgR0xPQkFMIEZPUiBMRUdBTCBQRVJTT05TIC0g
MjAxNjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMQpuzfdd6mEA4MK3oa1YELp6Ibt
yGi5IDROJm6hMxgf6ExUoOVURGuy1OLJwyz5lWFU1Rp6l22Hlb2TxJyMOHQYCjyNIT9GVtyYU4RI
oN4a7Ms+88BDtvLZ0mSEPG1Uy6qyA6ZrvJgi8kP4P56dT2xWimOv1tRmXcOLNWsbMP8ZxB6ozW
2D/C/YrU+MUADm0yyF6D9REvuRNWDpdLJd2Y6B+9JiAXRWIlB2wme9UNAzK3zfDQkMygSZxMFSB
6YKIDGBTApu3NpxMDD/nurMb4jAoCcHgyXZuWJg+LP3/Yjqg8VgHA19Vx/kKol78OtxZD7dnC1H5
sRIEnqr3R9Lxy0Dzw1PwPWTbwI33k2aJv5LZUkdnTZYuDVTMYTgvo0lNrGZtDl6R4tGKs/AcesZX
N6/aNayyKtmSjlGNvdDTZNAS4Iu8mTBnOvuYTCZEYwyYnWMdMchr4kQUQKdvTQuz5hp1Uu6R5HHr
B4NYQJgH3YFsvJPtGZxxsD8nzc9DDQxanp4FiCuYSFyOKKxYkwrltjsf7cFExOIP3MnVo9sa79Z
fJKpIXbZX5IQPeohNdleOOAchcd+9ojmki1ag+64rzPISBliYeiBMOOa4BjZPb+edzKfiulIDcGK0
2PoMy9sd0l4KBryv1X6gsVnNwg88CYZ1Z2nV1+fikW+asATNAgMBAAGjggLjMIIC3zASBgNVHRMB
AIBECDAGAQH/AgEBMB0GA1UdDgQWBBSAld9xSc/Ua9ozhtEPscXdZUyEXjCCAUEGA1UdIwSCATgw
ggE0gBTShJdETdmI7mvlv1KAsyIlm4sYhKGCARCkggEMMIIBCDELMAKGA1UEBhMCRVMxDzANBgNV
BAgMBk1BRFJJRDEPMA0GA1UEBwwGTUFEUklEMTowOAYDVQQLDDFzZWUgY3VycmVudCBhZGRyZXNz
IGF0IHd3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzMScwJQYDVQQLDB5HTE9CQUwgQ0hBTUJFUlNJ
R0dgUk9PVCAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0MzI4NzEYMBYGA1UEYQwPVkFURVMtQTgyNzQz
Mjg3MRswGQYDVQQKDBIBQyBDQU1FUkZJUk1BIFMuQS4xIzAIBgNVBAMMHkdMT0IBTCBDSEFNQkVS
U0lHTiBST09UIC0gMjAxNoIIEQhxWldLpE0wegYIKwYBBQUHAQEEbjBsMEIGCCsGAQUFBzAChjZo
dHRwOi8vd3d3LmNhbWVyZmlybWEuY29tL2NlcnRzL2FjX2NhbWVyZmlybWEtMjAxNi5jcnQwJgYI
KwYBBQUHMAGGGmh0dHA6Ly9vY3NwLmNhbWVyZmlybWEuY29tMA4GA1UdDwEB/wQEAwIBBjAdBgNV
HSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwPgYDVR0gBDcwNTAzBgRVHSAAMCswKQYIKwYBBQUH
AgEWHWh0dHBzOi8vcG9saWN5LmNhbWVyZmlybWEuY29tMHoGA1UdHwRzMHEwNqA0oDKGMGh0dHA6
Ly9jcmwuY2FlZXJmaXJtYS5jb20vYWNlY2FlZXJmaXJtYS0yMDE2LmNybDA3oDWgM4YxaHR0cDov
L2NybDEuY2FlZXJmaXJtYS5jb20vYWNlY2FlZXJmaXJtYS0yMDE2LmNybDANBgkqhkiG9w0BAQsF
AAOCAgEAF7nei08N/20tXbw8UJTA+TY6Sr1Jg87KhL5BaobU3+fCDZEPnuOvyztMBMMUaQcLnH6I
eIG/M2pASM6xj/Mo6dURh+azLyso8YDQOp4EE2E3TJ5lmFUT5FyCNn15/ww0ECqYPLu7X+kNFQD
bzrYGG3Uv/YnzvvnM4ynN60InLILWOquhxiLa8FyvOwN4aGlu25ybApU7kO0K/qBuZnl8BPojtHa
hipjQmg/bD7GwvG2AAISrEN+dCw2klgw8u5gRmS5yES57KlnJ5WkObQb0eafecENKZQ6PYUDflbC
dTIXUDE4uoqU8SB2HRHL837Pbkor25z87hANqjWcvz5RpdZYjprsh7VdyQWgx+Vndy11vvbA52nUQ
P26AS3zPx+1CSd7AmUCeffu+XU3Hl2wOIa/fguuVwjtswGEK6lUZ+4jc2wXfCNcsmIoA9Agit0IR
7sl6+t38zT0PsuJ4MrHuADLWTNB2vtaXUXPwU8Rqngka2KeUp2jGD0/1MVzlqZDricRkY07VdgJa
xnKQH5C05ACIMreH1P8IgxJpF132XD67xL7ATe6sPxxOMX++/yvn+TQKKFCsYIzIYxJgcnuljNbP
rHR35JdJxNT6SltocWtJvLgWWMU3By6rNu/nrCoH2MIbuX5LZb4TZmZpNWehEGLtxjc/e+7rl4qD
6Cu9V/0=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN:	*AC CAMERFIRMA - 2016*
Issuer O:	*AC CAMERFIRMA S.A.*
Issuer 2.5.4.97:	*VATES-A82743287*
Issuer SERIAL NUMBER:	*A82743287*
Issuer OU:	*AC CAMERFIRMA - 2016*
Issuer OU:	*see current address at https://www.camerfirma.com/address*
Issuer L:	*MADRID*
Issuer ST:	*MADRID*
Issuer C:	*ES*
Subject CN:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*
Valid from:	*Thu Apr 14 16:58:36 CEST 2016*
Valid to:	*Wed Feb 08 15:58:36 CET 2040*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C4:29:BB:37:DD:77:A9:84:03:83:0A:DE:86:B5:60:42:E9:E8:86:ED:C8:68:B9:20:34:4E:26:6E:A1:33:18:1F:E8:4C:54:A0:E5:54:44:6B:B2:D4:E2:C9:C3:2C:F9:95:61:54:D5:1A:7A:23:6D:87:95:BD:93:C7:7C:8C:38:74:18:0A:3C:8D:95:3F:46:56:DC:98:53:84:48:A0:DE:1A:EC:CB:3E:F3:C0:43:B6:F5:19:D2:74:84:3C:6D:54:CB:AB:B2:A8:0E:AD:67:3B:C9:82:2F:24:3F:83:F9:E9:F4:F6:C5:68:A6:3A:FD:6D:46:65:DC:38:B3:56:B1:B3:0F:F1:9C:41:EA:8C:D6:D8:3F:C2:FD:8A:D4:F8:C5:00:0E:7D:32:C8:5E:83:F5:11:2F:B9:13:56:0E:97:4B:D5:DD:98:E8:1F:BD:26:20:17:45:69:65:24:1D:B0:99:EF:54:34:0C:CA:DF:37:C3:42:43:32:83:96:71:30:54:81:E9:82:A5:0C:60:53:02:9B:B7:36:9C:4C:0C:3F:E7:BA:B3:1B:E2:30:28:09:C1:E0:C9:76:6E:58:98:3E:2C:FD:FF:62:3A:A0:F1:58:07:03:5F:55:C7:F9:0A:A0:8E:FC:3A:DC:59:0F:B7:67:0B:51:F9:B1:19:44:9E:AA:F7:47:D2:F1:CB:40:F3:C3:53:F0:3D:64:DB:C0:8D:F7:93:66:89:BF:92:D9:52:47:67:4D:96:2E:0D:54:CC:61:38:2F:A3:49:4D:AC:66:6D:0E:5E:91:E1:F1:8A:B3:F0:1C:7A:C6:57:37:AF:DA:35:AC:B2:2A:D9:92:96:31:8D:BD:D0:FB:64:D0:12:E0:8B:BC:99:30:67:3A:FB:98:4C:26:44:63:0C:95:9D:63:1D:31:C8:6B:E2:44:14:40:A7:6F:4D:0B:B3:E6:1A:75:52:EE:91:E4:71:EB:07:83:58:40:9A:87:DD:51:6C:BC:93:C6:67:1C:6C:0F:C9:E3:CD:CF:43:0D:0C:5A:8A:9E:05:88:2B:98:48:5C:8E:28:AC:58:93:0A:C8:B6:3B:1F:ED:C1:44:C4:E2:0F:DC:C9:EF:56:8F:6C:6B:BF:59:7C:92:A9:21:76:D9:5F:92:10:3D:EA:21:35:D2:1E:38:E0:1C:85:C7:7E:F6:88:E6:92:2D:5A:83:EE:B8:AF:33:DF:48:19:62:61:E8:81:30:E3:9A:E0:18:D9:3D:BF:9E:77:32:9F:B8:99:43:70:62:B4:D8:FA:0C:CB:DB:1D:D2:5E:0A:06:B8:EF:D5:7E:AA:81:59:CD:C2:0F:3C:09:86:75:67:69:D5:D7:E7:E2:91:6F:9A:B0:04:CD:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 1*
Subject Key Identifier	*80:21:DF:71:F1:EF:D4:6B:DA:33:86:D1:0F:BE:C5:DD:65:4C:84:5E*
Authority Key Identifier	*D2:84:97:44:4D:D9:88:EE:7C:25:BF:52:80:B3:29:48:9B:8B:18:84*

Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma-2016.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma-2016.crl* *http://crl1.camerfirma.com/ac_camerfirma-2016.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*4D:20:C9:51:E1:34:89:3B:C5:90:1B:FA:F8:E2:40:A5:BE:7D:00:59:6D:D3:1C:40:42:92:52:F2:E0:4F:8B:46*

X509SubjectName

Subject CN:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-07-21T00:00:00Z

11.13.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2*

11.13.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.13.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*
Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*gCHfcfHv1GvaM4bRD77F3WVMhF4=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

11.13.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2*

11.13.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.13.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject O:	*AC CAMERFIRMA S.A.*

Subject 2.5.4.97:	*VATES-A82743287*
Subject SERIAL NUMBER:	*A82743287*
Subject OU:	*AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*
Subject OU:	*see current address at https://www.camerfirma.com/address*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*gCHfcfHv1GvaM4bRD77F3WVMhF4=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2016-06-23T22:00:00Z*

11.13.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2*

11.14 - Service (granted): Qualified Certificates issued by Camerfirma Corporate Server II - 2015

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by Camerfirma Corporate Server II - 2015*

Name *[es]* *Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7070637242797760822*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIkzCCBnugAwIBAgIIYb/zHEibsTYwDQYJKoZIhvcNAQELBQAwga4xCzAJBgNVBAYTAkVVMUMw
QQYDVQQHEzpNYWRyaWQgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29t
L2FkZHJlc3MpMRIwEAYDVQQFEwlBODI3NDMyODcxGzAZBgNVBAoTEkFDIENhbWVyZmlybWEgUy5B
LjEpMCcGA1UEAxMgQ2hhbWJlcnMgb2YgQ29tbWVyY2UgUm9vdCAtIDIwMDgwHhcNMTUwMTE1MDky
MTE2WhcNMzcxMjE1MDkyMTE2WjCB0zELMAkGA1UEBhMCRVMxFjAUBgNVBAsMDUFDIENBTUVSRkIS
TUExGzAZBgNVBAoMEkFDIENhbWVyZmlybWEgUy5BLjESMBAGA1UEBRMJQTgyNzQzMjg3MLswSQYD
VQQHDEJNYWRyaWQgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgaHR0cHM6Ly93d3cuY2FiZXJmaXJt
YS5jb20vYWRkcmVzcykxLjAsBgNVBAMMJUNhbWVyZmlybWEgQ29ycG9yYYXRlIFNlcnZlciBJSSAt
IDIwMTUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC3ndKNpFiuVq9v+15dRoT9oVkg
wEfDdsPwdL y0R+cM5M0k35zEiU/+hqEMbQmcwosAh6f6AskkXasqb+SMbMJivXbDyNlLzGzsoP0
uz3btHM7oN3yHXDhhd1NGNocP54Wehe9+RE3WP0yEEo+D2YmMwUHuv4KiXtveiPksv+Xkkz5auqp
pPMaYlD6y49AEsGY2zOEUl8PO4+tOxUKhvsiMuW817vH3VdmMwOjRe0SdYAiYLQIyqJGNdEo3u+
fw8UXxaJSRXbmF++jUn5DvdzWWNAxxwAKy95EPlpLQsc/7t2W2ntoELPHGJk4V+/yA0d2oILEqBAD
kRtP2HiC0wly+zp7OGmtifbqLrVjmo/mLP3zpmYbpUubrHY0rlW6wo5FZLcT1vcAxFjxLWVIE
LPpTeb0uHvsTTp97thA1Oqqwoqs5FWJHFI9dzXzFLO0L X/4ug9L2WxmvWW0C4CcPtnhp0aNE/G
gAw6lMx7bjZeDXxxQnUDEE/mAqOHRUCnvRUSKVbuBBE0oz5fz3nUwcWVVgrm/jkgqTX4EqnZc+yB
mKV6hFEYV+1oVh7kzNN4Hg7nzGuByS7eCuBEwULFhfU/ja1Bu9EggndJ3CV0XCWIAXVhJnPNPi6y4
W11jLJ7XSGSz3sCh21g0Cpgi2pXHGDB65Jc/QJHZ5ZaHCrzFnwIDAQABo4ICjDCCAogwEgYDVR0T
AQEBAgwBgEBwIBAjAdBgNVHQ4EFgQUY+mw8FYAaGWwIWwOXNcZUl0NGUwgcMGA1UdIwSB2zCB
2IAU+SSsD7K1+HnA+mCIG8TZTQKeFxmhgbSkgbEwga4xCzAJBgNVBAYTAkVVMUMwQQYDVQQHEzpN
YWRyaWQgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3Mp
MRIwEAYDVQQFEwlBODI3NDMyODcxGzAZBgNVBAoTEkFDIENhbWVyZmlybWEgUy5BLjEpMCcGA1UE
AxMgQ2hhbWJlcnMgb2YgQ29tbWVyY2UgUm9vdCAtIDIwMDdCCQCZ2kI+pLGu2jB6BggrBgEFBQcB
AQRuMGwwQgYIKwYBBQUHMAKGNmh0dHA6Ly93d3cuY2FiZXJmaXJtYS5jb20vY2VydHMvcm9vdF9j
aGFtYmVycy0jMDA4LmNydDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3AuY2FiZXJmaXJtYS5jb20w
DgYDVR0PAQH/BAQDAgEGMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYIKwYBBQUHAwEw
PgYDVR0gBDcwNTAzBgRVHSAAMCswKQYIKwYBBQUHAgEWHWhtdHBzOi8vcG9saWNSLmNhbWVyZmly
bWEuY29lMHgGA1UdHwRxMG8wNaAzoDGGL2hddHA6Ly9jcmwuY2FiZXJmaXJtYS5jb20vY2hhbWJl
cnNyb290LTIwMDguY3JsMDagNKAyhjBodHRwOi8vY3JsMS5jYW1lcmZpcm1hLmNvbS9jaGFiYmVy
c3Jvb3QtMjAwOC5jcmwwDQYJKoZIhvcNAQELBQADggIBAKhqaZwalwf89f4wPrjfcE/lrsHdx8+q9
RG46ouBXbTJMqXjwszXOZSL43Dgs3GaVuMPIMWOG7CK0193mAr+HWtrd9ACFTvPBxPgAmzÅRHy
Eto+/6wt0WZ9HowNw0aUg3ZAkhlvMRPVou8PvtVukqj2lGKlh3hRdrbHwYwwmKKNlWBoC9gWk3mTYU
zfNt/KTzQCCl5+s6YDa+XInMLWaGd/pE/e++a22vY24cv7kN3NAFMjAMELPwh9iczLoPX8B52r+G
gwpKY0c0hZdVTii6psL/Q+BenyMlh+6lHRBOlTCSRtNi16o7H8fRqCY2wyQt7N+EmdY1DhvECC1n
Ib0nIx1bSAWdcVwPVrjQ/vsAxPNc3SGie/Xnanm3azAgFspzeuAhxxG0VKOvtPBnPQNsQ6eK66d+I
rWRsfa6aYbEIKv4sn5o4HpBWDobfzrNbqj0uiM6JkT+DxXo5UK7t2q75KCIimTrAuPcZ5wEtZ
ISLvZ34BodlHIL2xKb3Vww7K2FE1QaNstQkGbU/k++B9/+vV3H57vzskObdFWeWKSCpxIil4vZwIIH
17znWU+O2WIY1F0aO9zp3E7qwfmYT4MJ38NF9R7FSlxRlgVc1uU/Hu/iyUU4N1O6F3VdXP2Y+tgLF
ZLYV4kApfXk5l9h94dgKytVcIpvS6yVpLf0NPnlCNOxy

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Chambers of Commerce Root - 2008*

Issuer O: *AC Camerfirma S.A.*

Issuer SERIAL NUMBER: *A82743287*

Issuer L: *Madrid (see current address at www.camerfirma.com/address)*

Issuer C: *EU*

Subject CN: *Camerfirma Corporate Server II - 2015*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

Valid from: *Thu Jan 15 10:21:16 CET 2015*

Valid to: *Tue Dec 15 10:21:16 CET 2037*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B7:9D:D2:8D:A4:5B:9F:56:AF:6F:FB:5E:5D:46:84:FD:A1:59:20:C0:47:C3:76:C3:F0:D0:BC:B4:47:E7:8C:E4:C3:A4:DF:9C:C4:8A:5F:FE:86:A1:0C:6D:09:9C:BE:8B:00:87:A2:3C:88:0B:24:91:76:AC:AA:1F:92:31:B3:08:8E:F5:DB:0F:23:48:2D:E1:B3:B2:83:F4:BB:3D:DB:B4:73:3B:A0:DD:F2:1D:70:E1:85:DD:4D:18:DA:1C:3F:9E:16:7A:17:BD:F9:11:37:58:FD:32:10:4A:3E:0F:66:26:33:05:07:BA:FE:0A:89:7B:6F:7A:23:E4:B2:FF:97:92:4C:F9:6A:EA:A9:A4:F3:1A:62:50:FA:CB:8F:40:12:C1:98:DB:33:84:50:8F:0F:3B:8F:AD:3B:15:0A:86:FB:22:32:E5:BC:D7:BB:C7:DD:57:66:33:03:A3:45:ED:12:75:80:22:60:B4:08:8B:2A:89:18:D7:44:A3:7B:BE:7F:0F:14:5F:16:89:49:15:E1:98:5F:A3:52:7E:43:BD:DC:D6:58:D0:31:C7:00:0A:CB:DE:44:3E:5A:4B:42:CC:7F:EE:DD:96:DA:7B:68:10:B3:C7:18:99:38:57:EF:F2:03:47:76:A2:52:C4:A8:10:03:91:1B:4F:D8:78:82:D3:09:72:FB:3A:7B:38:69:A3:B5:F8:DB:A8:BA:D5:8E:6A:3F:98:B3:F7:CE:99:98:6E:95:2D:B9:BA:C7:89:8D:2B:95:6E:B0:A3:91:59:2D:C4:D4:BD:C0:31:16:3C:4B:59:52:04:2C:F8:E7:4D:E6:CE:B8:7B:E8:25:36:FD:EE:B8:40:D4:EA:AA:C2:8A:B9:15:62:47:14:8F:62:77:35:F3:14:B3:B4:2D:7F:F8:BA:02:3D:2D:95:B1:9A:F5:96:D0:EE:02:78:FB:67:86:9D:1A:34:4F:C6:80:0C:3A:94:CC:7B:6E:36:5E:0D:7C:71:42:75:03:10:4F:E6:02:A3:87:45:40:A7:BD:15:12:29:56:EE:04:11:34:A3:3E:5F:CF:79:D4:C1:C5:95:56:0A:E6:FE:39:20:A9:35:F8:12:A9:D9:7B:EC:81:98:A5:7A:84:51:18:57:ED:68:56:1E:E4:CC:D3:78:1E:0E:E7:CC:6B:81:C9:2E:DC:0A:E0:44:C1:42:C5:85:F5:23:6B:50:6E:F4:4A:A0:9D:D2:77:09:5D:17:09:62:00:5D:58:49:9C:F3:4F:8B:AC:B8:5B:5D:63:2C:9E:D7:48:64:B3:DE:C0:A1:DB:58:34:1A:98:22:DA:95:C7:18:30:7A:E4:97:3F:40:91:D9:E5:96:87:0A:BC:C5:9F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D:08:34:65*

Authority Key Identifier *F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19*

Authority Info Access

http://www.camerfirma.com/certs/root_chambers-2008.crt

http://ocsp.camerfirma.com

Extended Key Usage *id_kp_clientAuth - id_kp_serverAuth*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://policy.camerfirma.com

CRL Distribution Points

http://crl.camerfirma.com/chambersroot-2008.crl

http://crl1.camerfirma.com/chambersroot-2008.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *66:EA:E2:70:9B:54:CD:D1:69:31:77:B1:33:2F:F0:36:CD:D0:F7:23:DB:30:39:ED:31:15:55:A6:CB:F5:FF:3E*

X509SubjectName

Subject CN: *Camerfirma Corporate Server II - 2015*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time *2017-08-16T01:00:00Z*

11.14.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

11.14.2 - History instance n.1 - Status: withdrawn

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by Camerfirma Corporate Server II - 2015*

Name *[es]* *Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015*

Service digital identities

X509SubjectName

Subject CN: *Camerfirma Corporate Server II - 2015*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

X509SKI

X509 SK I *Y+nw8FYAaGWwIWwOXNcZCJ0INGU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Status Starting Time *2017-07-21T00:00:00Z*

11.14.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2

11.14.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.14.3 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by Camerfirma Corporate Server II - 2015

Name [es] Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015

Service digital identities

X509SubjectName

Subject CN: Camerfirma Corporate Server II - 2015

Subject L: Madrid (see current address at https://www.camerfirma.com/address)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject OU: AC CAMERFIRMA

Subject C: ES

X509SKI

X509 SK I Y+nw8FYAaGWwIWwOXNcZCJ0INGU=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time *2016-06-30T22:00:00Z*

11.14.3.3 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2*

11.14.3.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.14.4 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by Camerfirma Corporate Server II - 2015*

Name *[es]* *Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015*

Service digital identities

X509SubjectName

Subject CN: *Camerfirma Corporate Server II - 2015*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

X509SKI

X509 SK I *Y+nw8FYAaGWwIWwOXNcZCJ0INGU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-23T22:00:00Z*

11.14.4.5 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2*

11.15 - Service (granted): Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016*

Name *[es]* *Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES - 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2579987068168128523*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIUpjCCB46gAwIBAgIII830kbNDSAswDQYJKoZIhvcNAQELBQAwggEMMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFk
ZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9G
IENPTU1FUkNFIFJPT1Qgl.SAyMDE2MRIwEAYDVQQFEwIBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVT
LUE4Mjc0MzhNzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSKwJwYDVQQDCBDSEFNQkVS
UyBPRlBDT01NRVJDRSBST09UICDgMjAxNjAeFw0xNjA0MTgxNTQzNTRaFw00MDAzMTMxNTQzNTRa
MIIBFjELMAkGA1UEBhMCRVMxDzANBgNVBAgMBk1BRFJlRDEPMA0GA1UEBwwGTUFEUklEMUIwQAYD
VQQLDDlzZWUgY3VycmVudCBhZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2Fk
ZHJlc3MxKjAoBgNVBAsMIUFDIENBTUVSRkJSTUEgRk9SIFdFQlNJVEVTIC0gMjAxNjESMBAGA1UE
BRMJQTgyNzQzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI5NDMyODcxGzAZBgNVBAoMEkFDENBTUVS
RkISTUEgUy5BLjEqMCgGA1UEAwwhQUMgQ0FNRVJGSVJNQSBGT11gV0VCU0lÚRVMgLSAyMDE2MIIC
IjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA0zVWn12uemc/1Ã+0V7U+aPDWi8vowmzAaA9v
qeEZzTdBNvZJ34Sra9wsAySJlIAXPOWCX/YHJwJMvduhyl5VOG8O7MeOgjg6XP4ps5P2FpyRgI
cGB/SnWnbHDrJzFN2HT7FsitPibgm9TmGSpTHEi6vkOSCnD2xVI9C+qMaQKSqPkMostSvPnS/5I
Dh5opYxJJ0o+7r565xKnFVxPiUJAIxmizk/7Fb2qCHrKHU4SaDCnxNK0hyw80A1iiu8Abq5U0AtF
IVkrlw+3U6FGy45Mad2wiQfLno4TDSf/qOxetcwtRq7+WwSUO4iCrGplShjYJNiEvIV4QzqmHgVG
L8TldY13WRq+7GgKJZ0P726R8XtSMTiQ2TaMdzkxvAgGBAafPPOLKB7ZLpmGSTmY80sa9JdSVFg
L0k+CEIIAtPcmVuoosxDXb5yCnZFE5MMWsI15xDqIfyX7YAvWO9Dhur5LkoH8nmxmfiEWcXUcyN
DxPFVY+Q/L4gYXSER9lIS+lQXLmoHfyZvUnSkqfVp3Pz7elzjNnhGx3xWicDRfcxkjjpYVsidJfx
h/7XHcMapgkEhuUVpqUSzcJgyb98lUKv8taZF6YqoCs7DLjtUcsBwyGQltCinYvL58TqF7XYfEqK9
8psOD8B8ZoJSKgEtDe98F9UzalhbTUUYf158vECAwEAAaOCAvwwggL4MBIGA1UdEwEB/wQIMAYB
A8CAQwHQYDVR0OBBYEFOyVMzxwNKxnFgiCzZBvFSeL.HdMIIBRQYDVR0jBIIBPDCCATiAFJ4e
ZU8+V/WrfZbGi9+zNW1K6J6LoYIBFKSCARAwggEMMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFE
UklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3
LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9GIENPTU1FUkNFIFJP
T1Qgl.SAyMDE2MRIwEAYDVQQFEwIBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVTLUE4Mjc0MzA4NzEb
MBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSKwJwYDVQQDCBDSEFNQkVSUyBPRlBDT01NRVJD
RSBST09UICDgMjAxNolINJotoYIGsrMwgYMGCCsGAQUFBwEBBHcwdTBLBggrBgEFBQcwAoY/aHR0
cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9jaGFtYmVyc29mY29tbWVyY2Vyb290LTIwMTYu
Y3J0MCYGCCsGAQUFBzABhhpodHRwOi8vb2NzcC5jYW1lcmZpcm1hLmNvbTAOBgNVHQ8BAf8EBAMC
AQYwEwYDVR0lBAwwCgYIKwYBBQUHAwEwPgYDVR0gBDcwNTAzBgRVHSAAMCswKQYIKwYBBQUHAgEW
HWh0dHBzOi8vcG9saWN5LmNhbWVyZmlybWEuY29tMIGOBgNVHR8EgYYwgYMwP6A9oDuGOWh0dHA6
Ly9jcmwuY2FlZXJmaXJtYS5jb20vY2hhbWJlcnNvZmNvbWJlcmNlcm9vdC0yMDE2LmNybDBAoD6g
PIY6aHR0cDovL2NybDEuY2FlZXJmaXJtYS5jb20vY2hhbWJlcnNvZmNvbWJlcmNlcm9vdC0yMDE2
LmNybDANBgkqhkiG9w0BAQsFAAOCAgEAcH4uc9lGrFngS3POapuNrKSeAg93Ib7Oj+80KwhfAbF1
duHp75R6LN5jqrmmCAIf11Uq5Pw9UZWKGbiQ/3tV8UpeGyrJ2R/ebVSjm3+ng7VNYPl4D0F+zWR
LhkTe5vFAXUFU0bJSaX1LQMt2N8E24AIbejDcz1dY4dFs0L+Vm0SwNoG+mSEeiT11aYMcrq78WLN
SIU00lcFLnufEm57w73XAoCx44LY0BvjP2UruDIOUZ5Bg9rqM+FK0zF8BkXOGRbGhv2W2UM6MXVq
WFcZ4thnScWS5dam0LdcXxruDJ7zflzlR7W3NkaOU3QbbG6V6tL4V342Hae+GVgLeF4PlRGRbtMM
MTiXnbWhAad+gd3MAycdNKcMmbE99i2jqDgfS42taSlvH4Phule0sXwf5wjRRCfIHlslZ+Cux3TD
+TJlI372u2n7LEg4G5wgIzrDbLqWCYrYwteXcHHDM1oQizuAaEamn1ZqNsu4V2g4LmXp+ynz7l61
0TC288S+IF6p2brSrhbDaADk4D0v4S2kdTogxkMePfCHeiTsYjb+5I9pOQVW8qY3lrr9sRH/2SUu
OcO5V03XZRMFg5/I70rwAgHjuy7Lx8WCUbIu1yPP63PmrKAu9CQI2FXxI/A7i3U3EzCnBI+mzAk1
/eUfGPYgRqtlLwNZo0OhpVHZwhMNHtw=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA FOR WEBSITES - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Valid from: *Mon Apr 18 17:43:54 CEST 2016*

Valid to: *Tue Mar 13 16:43:54 CET 2040*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D3:35:56:9F:5D:AE:7A:67:3F:D4:0F:B4:57:B5:3E:68:F0:D6:8B:CB:E8:C2:6C:C0:68:0F:6F:A9:E1:19:CD:37:41:36:F6:49:DF:84:AB:6B:D9:70:B0:0C:92:26:52:00:5C:F3:96:09:7F:D8:1E:22:70:7C:CB:DD:BA:58:72:23:95:4E:1B:C3:BB:31:E3:A0:8A:0E:97:3F:8A:79:3F:61:69:C9:18:08:78:60:7F:4A:65:A7:6C:70:EB:27:31:4D:D8:74:FB:16:C8:8F:7E:26:E0:9F:D4:E6:19:2A:53:1D:F1:22:EA:F9:0E:E4:29:CE:DB:35:48:F4:2F:AA:31:A4:0A:4A:A3:E4:32:8B:2D:4A:F3:E7:4B:FE:48:0E:1E:68:A5:8C:49:27:4A:3E:EE:BE:7A:E7:12:A7:15:5C:4F:89:42:40:23:19:A2:CE:4F:FB:15:BD:AA:08:7A:CA:1D:4E:12:68:30:A7:C4:D2:B4:87:2C:3C:D0:0D:62:8A:EF:00:6E:AE:54:D0:0B:45:21:59:2B:97:0F:B7:53:A1:46:CB:8E:4C:69:DD:B0:89:07:CB:9E:8E:13:0D:27:FF:A8:EC:5E:B5:CC:2D:46:AE:FE:5B:04:94:3B:88:82:AC:6A:48:E6:18:D8:24:D8:84:BE:55:78:43:3A:A6:1E:05:46:2F:C4:E5:75:88:B7:59:1A:BE:EC:68:0A:25:9D:0F:EF:6E:91:F1:7B:52:31:38:90:D9:36:8C:77:39:31:BC:08:06:04:06:9F:3C:F3:8B:28:1E:D9:2E:99:86:49:39:98:F3:4B:1A:F6:22:5D:49:51:60:2F:49:3E:08:42:09:02:D3:DE:99:5B:A8:A2:CC:43:5D:BD:F2:0A:76:45:13:93:0C:5A:82:75:E7:10:EA:21:FC:97:ED:8E:2F:58:EF:43:D2:EA:F9:2E:4A:07:F0:99:E7:C6:67:E2:11:67:17:51:CC:8D:0F:13:C5:55:8F:90:FC:BE:20:61:74:84:47:D2:25:4B:E9:50:5C:B9:A8:1C:8C:99:BD:49:D2:92:A7:D5:A7:73:F3:EF:39:73:8C:D9:E1:1B:1D:F1:5A:27:03:45:F7:31:92:38:E9:61:5B:22:74:97:F1:87:FE:D7:1D:C3:1A:A6:09:04:86:E5:15:A6:A5:12:CD:C2:60:C9:BF:7C:21:42:AF:F2:76:45:E9:8A:A8:0A:CE:C3:2E:3B:49:72:C0:70:C8:64:08:B4:28:A7:62:F2:F9:F1:3A:85:ED:76:1F:12:A2:BD:F2:9B:0E:0F:C0:7C:66:82:52:2A:01:2D:0D:E9:7D:F0:5F:54:CD:A9:61:6D:35:14:61:F2:39:F2:F1:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *EC:95:33:3B:71:C0:D2:B1:9C:58:23:0B:36:41:BC:54:9E:2C:92:1D*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access

http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt

http://ocsp.camerfirma.com

Extended Key Usage *id_kp_serverAuth*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://policy.camerfirma.com

CRL Distribution Points

http://crl.camerfirma.com/chambersofcommerceroot-2016.crl

http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *93:7D:7D:5D:0B:7F:B7:DB:03:93:99:BC:0B:67:0C:C2:03:C7:AB:4E:33:2F:AE:45:3C:C3:8E:C1:88:DD:EA:2B*

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR WEBSITES - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *7JUzO3HA0rGcWCMLNkG8VJ4skh0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-03-15T01:00:00Z*

11.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

11.16 - Service (granted): Qualified timestamps issued by AC CAMERFIRMA TSA - 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by AC CAMERFIRMA TSA - 2016*

Name *[es]* *Sellos de tiempo cualificados emitidos por AC CAMERFIRMA TSA - 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1564901409084605058*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJIDCCB3ygAwIBAgIIFbeliIT/AoIwDQYJKoZIhvcNAQELBQAwggEMMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUkUiEMQ8wDQYDVQQHDAZNQUROSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFk
ZHUlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHUlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9G
IENPTU1FUkNFIFJPT1QgLSAyMDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVT
LUE4Mjc0MzI4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSkwJwYDVQQDDCBDSEFNQkVS
UyBPRiBDT01NRVJDRSBST09UIC0gMjAxNjAeFw0xNjA0MTQxMDOyMDIaFw00MDAzMDkxMDOyMDIa
MIIBBDELMAkGA1UEBhMCRVMxDzANBgNVBAgMBk1BRFJRDEPMA0GA1UEBwwGTUFE1kIEMUIwQAYD
VQQLDDlzZWUgY3VycmVudCBhZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2Fk
ZHUlc3MxITAfBgNVBAsMGEFDIENBTUVSRkkiSTUEgVFNBICO gMjAxNjESMBAGA1UEBRMJQTgyNzQz
Mjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkiSTUEgUy5B
LjEhMB8GA1UEAwwYQUMgQ0FNRVJGSVJNQSBUU0lEgLSAyMDE2MIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEApsy/JRhXjglywJSILjY9T7Pjsb1pHW97xc/AJkeHpezI17NREESfWb20EEnS
amO3XrIbww4iMuvXVJ1T2w1+bQLT8P4tmG1jKkRHC6oHEQFn1mcE3VvxUNbvbUPrkPd57raGYY/
6aT4durAOARVA6XkWQKcBIT9lPpNrw/y1IO/HNrU23PgREn9gE7p48SlZ2kvkutBG8bA8JkDaDY
o8XiHqHN3x2YLJpPCo0wpXZGkhPuYLAd1acoqYGTzBBPcEbFjXOH2Y6upml3JOIFbmlyK66p4yGq
5zg36ndhV1yLA3hiarzJ6lP1QWPwPnzsiW0kSRjxi59N8ROppfzX13j7KHPF/PfZ1I1TP/cgXO6y
GxDh7BUJDQXAYRsCbFs8Wi3BXp8KEo1R6myJt7nmGSVq8m4sK+uoBuP7IZgnaMLwhoC wCZwBg3Ye
Nsnr2xTUcoAUuJeNnkrNIs6mZc6grJnttyWsL3jE7v9wzt+8lFU30FiHAszKMDRL3oM5tKiTtLj3
VSF4NjsSmYSmvNptYI03ST7E7s8no0w+Nc4+o51Fxqkhaqbos0Ub5STh897ca2/fyXZnwr1CSP
qZEsX2KXqzLfE17KmTSZLefVb+dedDO+M31c1hjf/gMeyOYuC9c5qLfgcj50EJFeqcHYIoLu5jZX
Jt9opnv5N3EbS/ECAwEAAaOCAvwwggL4MBIGA1UdEwEB/wQIMAYBAf8CAQIwHQYDVR0OBBYEFB5t
tcY/75JVXjf62/0QqrrZO04sMIIBRQYDVR0jBIIBPDCCATiAFJ4uZL/8+V/WrfZbGr9+zNW1K6J6L
oYIBFKSCARAwggFMMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFE1kIEMQ8wDQYDVQQHDAZNQURS
SUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFkZHUlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2Fk
ZHUlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9GIENPTU1FUkNFIFJPT1QgLSAyMDE2MRIwEAYDVQQF
EwlBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVT1LUE4Mjc0MzI4NzEbMBkGA1UECgwSQUMgQ0FNRVJG
SVJNQSBTLkEuMSkwJwYDVQQDDCBDSEFNQkVSUyBPRiBDT01NRVJDRSBST09UIC0gMjAxNoIlNJot
oYIGsrMwgYMGCCsGAQUFBwEBBHcwdTBLBggrBgEFBQcwAoY/aHR0cDovL3d3dy5jYW1lcmZpcm1h
LmNvbS9jZXJ0cy9jaGFtYmVyc29mY29tbWVyY2Vyb290LTIwMTYuY3J0MCYGCCsGAQUFBzABhhpo
dHRwOi8vb2N2zcC5jYW1lcmZpcm1hLmNvbTAOBgNVHQ8BAf8EBAMCAQYwEwYDVR0lBAwwCgYIKwYB
BQUHAwgwPgYDVR0gBDcwN7AzBgRVHSAAMCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vcG9saWN5LmNh
bWVyZmlybWEuY29tMIGOBgNVHR8EgYYwgYMwPKA6oDuGOWh0dHA6Ly9icmwuY2FtZXJmaXJhYS5j
b20vY2hhbWJlcnNvZmNvbWlcmNlcm9vdC0yMDE2LmNybDBAoD6gPIY6aHR0cDovL2NybDEuY2Ft
ZXJmaXJtYS5jb20vY2hhbWJlcnNvZmNvbWlcmNlcm9vdC0yMDE2LmNybDANBgkqhkiG9w0BAQsF
AAOCAgEAtHUD8qm6ZTS3YT5URykxatTAg54qexnRzK0rh3zsF7+GjNHmKVwQroXzVWnY83p9NUM7
L26d/yoz9qtsI7KOvuUBzNN6SDTz25jVrcO2NbPwe4Xafw15bzgDxnciEZtu7YMAOMxpBa3iFvW
/RK07LBQy3HYqYtxZPIgyuKoaEMeiH4v1P+3gAltRru7sV8zrYUMICT+jeCXBWydUsv3tb9YNOtz
l7vOUP7neqGqcpWYCvunsgctLryR7jp9qknLbEn+rjSy8VMahne1zNx5cAzzON0hMct1t8X0zlFV
qtEzxBP0kS0OaHyMBiZxW5VeU/CruYRZ0qhp9ZbpcpN7GlHQtDMSCjVnyq1IPMtHYhjOHEX1N8Ejj
9nd5gImnYcKDz74kU/TrmibEimK+0nS1AOVbLJHqmHBoiMkSDr/pAAk/HpL21tQSZ9D+=2HcNduo
5svFKdHeWTslcrxG7EhZKrqvbTdH5AViGZ6/w6QFWQzVJW7LXEYgMCmLBYisk41RegW0ZIQ3Y9NK
BcHWxqU4D+Vkh9eNdT1PPclzrtbABi6uNl+jADfiBnxl0FcNQpgKjrMxm/o+AUL9JpCGM+VIf3VM
ie/Nq1FinrgONVeBHXLv1S6XNwUHXS3lqDkz7MDeqrO4orY4BS/cJw5D6Zj5WCe+v7OAYITuA10li
M+YEt7Y=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT - 2016*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA TSA - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA TSA - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Valid from: *Thu Apr 14 12:42:09 CEST 2016*

Valid to: *Fri Mar 09 11:42:09 CET 2040*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:CC:BF:25:18:57:8E:09:63:C0:94:89:2E:36:3D:4F:B3:E3:B1:BD:69:1D:6F:7B:C5:CF:C0:26:47:87:A5:EC:C8:D7:B3:51:10:44:9F:59:BD:B4:10:49:D2:6A:63:B7:5E:B2:1B:C3:0E:22:32:EB:D7:54:92:35:4F:6C:35:F9:B4:0B:4F:C3:F8:B6:61:B5:8C:A9:11:1C:2E:A8:1C:44:05:9F:59:9C:13:75:6F:C5:43:5B:BD:B5:0F:AE:43:DD:E7:BA:DA:19:86:3F:E9:A4:FB:76:EA:C0:38:04:55:03:A5:E4:59:02:9C:04:84:FD:20:FA:4D:AF:0F:F2:23:53:BF:1C:DA:D4:DB:73:E0:44:49:FD:8E:01:3B:A7:8F:12:21:9D:A4:BE:4B:AD:04:6F:1B:03:C2:64:0D:A0:D8:A0:15:E2:7E:DA:87:37:7C:76:60:B2:69:3C:2A:34:C2:95:D9:1A:48:4F:B9:82:C0:77:56:9C:A2:A6:06:4F:30:41:3D:C1:1B:16:35:F4:1F:66:3A:BA:99:B4:DC:93:85:6E:62:32:2B:AE:A9:E3:21:AA:E7:38:37:EA:77:61:57:5C:8B:03:78:62:6A:BC:C9:E8:83:F5:41:63:F0:3E:7C:EC:89:6D:24:49:18:F1:8B:9F:4D:F1:13:A9:A5:FC:D7:D7:78:C9:EC:A1:CF:17:F3:DF:DA:5D:53:3F:F7:20:5C:1E:B2:1B:10:E1:EC:15:09:0D:05:C0:61:1B:02:6C:5B:3C:5A:2D:C1:5E:9F:0A:12:8D:51:EA:6C:89:B7:B9:E6:19:25:6A:F2:6E:2C:2B:EB:A8:06:E3:FB:7F:68:27:68:C2:F0:86:80:B0:09:9C:01:83:76:1E:36:C9:EB:DB:14:D4:72:80:14:B8:9C:CD:9E:4A:CD:D6:CE:A6:65:CE:A0:AC:99:ED:B7:25:AC:2F:78:C4:EE:FF:70:CE:DF:BC:94:55:37:D0:58:87:02:CC:CA:30:34:4B:DE:83:39:B4:AB:53:B4:B8:F7:55:21:78:36:3B:1F:4A:66:12:9A:F3:69:B7:F6:34:DF:C4:FB:13:BB:3C:C2:2D:30:F8:D7:38:FA:8E:75:17:1A:A4:85:AA:9B:A2:CD:09:69:2E:53:87:CF:7B:E9:AD:BF:7F:25:D9:BB:0A:E2:D4:24:8F:A9:91:2C:5F:62:97:AB:32:DF:13:5E:CA:99:34:99:2D:E7:D5:87:E7:5E:74:33:BE:33:7D:5C:22:18:DF:FE:A3:1E:C8:E6:2E:0B:D7:B9:A8:B7:E0:72:3E:74:10:91:5E:A9:C1:D8:22:82:EE:E6:36:57:26:DF:68:A6:7B:F9:37:71:1B:4B:F1:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access

http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt

http://ocsp.camerfirma.com

Extended Key Usage *id_kp_timeStamping*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://policy.camerfirma.com

CRL Distribution Points

http://crl.camerfirma.com/chambersofcommerceroot-2016.crl

http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BA:AE:2C:63:38:85:7D:50:20:0F:6F:73:DD:45:E6:5A:A2:D8:95:BE:D4:67:5B:6E:39:6B:72:22:E0:18:A9:B8*

X509SubjectName

Subject CN: *AC CAMERFIRMA TSA - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA TSA - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *Hm21xj/vklVeN/rb/RCqutk7Tiw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2018-03-15T01:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Camerfirma.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Camerfirma.aspx*

11.17 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES 2018

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES 2018*

Name [es] *Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES 2018*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1787353533750921228*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIIzCCB3+gAwIBAgIIGM30kbNDSAwwDQYJKoZIhvcNAQELBQAwggEIMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUkIEMQ8wDQYDVQQHDAZNQURSSUQxGjAYBgNVBAsMMXNlZSBjdXJyZW50IGFk
ZHIlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxIzAlBgNVBAsMHkNIQU1CRVJTIE9G
IENPTU1FUkNFIFJPT1QgMjAxODESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1B
ODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkISTUEgLUy5BLjEnMCUGA1UEAwwQ0hBTUJFUlMg
T0YgQ09NTUVSQ0UgUk9PVCAyMDE4MB4XDTE4MTAwNDA5MDAyM1oXDTOyMDgyODA5MDAyM1owggES
MQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFEUkIEMQ8wDQYDVQQHDAZNQURSSUQxQjBABgNVBAsM
OXNlZSBjdXJyZW50IGFkZHJlc3MgYXQgaHR0cHM6Ly93d3cuY2FtZXJmaXltYS5jb20vYWRkcmVz
czEoMCYGA1UECwwfQUMgQ0FNRVJGSVJNQSBGT1lgV0VCU0lURVMgMjAxODESMBAGA1UEBRMJQTgy
NzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkISTUEg
UySBLjEoMCYGA1UEAwwfQUMgQ0FNRVJGSVJNQSBGT1lgV0VCU0lURVMgMjAxODCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAL8WchVLf0lLG9ovFyq4QmKjMjau8LFx9UJU1iO3XP/ndyw
VwzPLJHeNXaXu8Sc4+1TxhbbDa9D3H3xbjvlanAp3IC8ZoxuMP0n9Qz4b55A3V29yyoTpCz1+em1
XUONylMr8MXPehuDO52Fmzg9iASKW33aIAqRyYI8LtkYZ7lBm7QW51IKjdvLsFm9/rG4lsADXjM+
ScNpbOBvnwceT4uIOG3J+dc5CpJ/8/B9BdTqYJMRaEIH4/LRX3G7+2z6LMrzXnMabJ2k1bFFar
NvdNiE1YM9UCIUS/0c57Le8jYVs7WuvKy2FCN7dHzFl7QB/aXBDrFYENIj7jruQ6p6lXx3kFyTwt
0ZdUQDS4QVioDSjNh51LtCxDXlRCh5nQEW7xWlnV7CCuhe8QeaI3BvdXAWRv3LbY/2zqvYgDqvyO
L+I6oxcHLr6tm3cxGAFRefc4+XE9Q23RFcFSv6Khj4P+W4fjJLeIr73A3Vw1UzZqPolERh3P59qW
KQ0lDXPnghuh598xZ1BbMfUqZ6z3rckKwkxIf9GJgZQgSwMICB8N4W1vwan1QXasIbFu7B2kG8T
GGrLkXbVXksseDBVKtwB8IHcdnGlW13aJ891xMa8AyrG9M8XrT/JXTVMx1htNQPNcuMc8nqafMl
Ln8NTEv4KujCxZQgu2z2Ow/hSUgtAgMBAAGjggL1MIIC8TASBgNVHRMBAf8ECDAGAQH/AgECMB0G
A1UdDgQWBBRQR1wvuhJ7X3Q4GwcSMfIoTKjv3jCCAUEGA1UdIwSCATgwggE0gBS1LIkgsq9Du5U9
wKGZA3VVNEiwHKGCARCkggEMMIIBCDELMAkGA1UEBhMCRVMxDzANBgNVBAgMBk1BRFJRDEPMA0G
A1UEBwwGTUFEUkIEMTowOAYDVQQLDDFzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd5dy5jYW1lcmZp
cm1hLmNvbS9hZGRyZXNzMScwJQYDVQQLDB5DSEFNQkVSUyBPRiBDT01NRVJDRSBST09UIDIwMTgx
EjAQBgNVBAUTCUE4Mjc0MzI4NzEYMBYGA1UEYQwPVkFURVMtQTgyNzQzMjg3MRswGQYDVQQKDBJB
QyBDQU1FUkZUk1BIFMuQS4xIzAlBgNVBAMMHkNIQU1CRVJTIE9GIENPTU1FUkNFIFJPT1QgMjAx
ODIGaQTdjUqcSYwgYKCCsGAQUFBwEBBHYwdDBKBggrBgEFBQcwAoY+aHR0cDovL3d3dy5jYW11
cmZpcm1hLmNvbS9jZXJ0cy9jaGFtYmVyc29mY29tbWVyY2Vyb290MjAxOC5jcnQwJgYIKwYBBQUH
MAGGGmh0dHA6L y9vY3NwLmNhbWVyZmlybWEuY29tMA4GA1UdDwEB/wQEAwIBBjATBgNVHSUEDDAK
BggrBgEFBQcDATA+BgNVHSAENzA1MDMGBFUdIAAwKzApBggrBgEFBQcCARYdaHR0cHM6L y9wb2xp
Y3kuY2FtZXJmaXltYS5jb20wgYwGA1UdHwSBhDCBgTBgTA+oDygOoY4aHR0cDovL2NybC5jYW1lcmZp
cm1hLmNvbS9jaGFtYmVyc29mY29tbWVyY2Vyb290MjAxOC5jcmwwP6A9oDuGOWh0dHA6L y9jcmwx
LmNhbWVyZmlybWEuY29tL2NoYW1iZXJzb2Zjb21tZXJjZXJvb3QyMDE4LmNybDANBgkqhkiG9w0B
AQsFAAOCAgEAmiKEwewzR4IaErxs1FP9alI1kK0zxf1v84CJyPkxYCNPCXdt1cwgqcgKxhjSIL1+
pPKGn7t01IhJprvJrBuCkerdmV+ZjlV+C331NSO42oS5cEZbmA8ls96+rxCzQFPmhqX3U+MuPbqT7
0MFa8QxxZaohXXTxpZqNw+DmSTJlpC49oA5kjaWbLiIwuWR8Sd6tL0N7KFaMStOLaK/Ha8TfC+
MEIARcrN7/gbRIJ6YZELC5bWygWhX/LquTz1IUxJBcdgIZmVT9oG9bXk7yxu9JYHr3BSBfweOS
EZArPEmX/0UzHHDid2+fRD78I8qHwRZRC0d14R+JN4VYKOmb4aZEanIF7NBzEfrLdBTTZ2505HUc
/kGEptkHdsG+oXQBQzcKs2HPYJTEzC3MbEMBtmvLYngtBgM2952+aVlvJLDvmcac3O7KJKZJYA
RhcNDyg8+ylb6Fj3aTxVs6oR/lqFcfodH0tYuQGeOljEHzCqTcYQwQvvEo6coMDJPIaB89Fb++e
L5XdHjAbAX+A3w/rVGq1hFhA3theJXDizItskW5lfhv9OFGS7O879eQ6eK57gphex9/zZ3teQko
3bH0oLmS4pEm4fQ60r72xlmOxDicMgxYiD4qKrVycvvKecgFTa3mW3aTgzSbqszz6RBgfMh6wLf8
n0ahjecD2R0=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT 2018*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT 2018*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Valid from: *Thu Oct 04 11:00:23 CEST 2018*

Valid to: *Thu Aug 28 11:00:23 CEST 2042*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BF:16:72:15:4B:7F:47:CB:1B:DA:2F:17:2A:B8:42:B9:CA:8C:C8:DA:BB:C2:C5:C7:D5:09:53:58:8E:DD:73:FF:9D:DC:B0:57:0C:CF:2C:91:DE:35:76:97:BB:C4:9C:E3:ED:53:C6:16:DB:0D:AF:43:DC:7D:F1:6E:3B:E5:6A:70:29:DC:80:BC:66:8C:6E:30:FD:27:F5:0C:F8:6F:9E:40:DD:5D:BD:CB:2A:13:A4:2C:F5:F9:E9:B5:5D:43:8D:CA:53:2B:F0:C5:CF:7A:1B:83:3B:9D:85:9B:38:3D:88:04:8A:5B:7D:DA:1C:0A:91:BD:82:3C:2E:D9:18:67:B9:41:99:34:16:E7:57:CA:8D:DB:CB:B0:59:BD:FE:B1:B8:22:C0:03:5E:33:3E:E5:C3:69:84:E0:6F:8B:07:1E:4F:8B:88:38:6D:C9:F9:D7:B9:0A:92:7F:F3:F0:7D:05:D4:EA:60:93:11:68:49:47:E3:F2:D1:5F:71:BB:FB:6C:7A:2C:CA:FF:AD:79:CC:6A:12:76:AE:4D:61:14:56:AB:36:F7:4D:88:42:18:33:D5:02:95:44:BF:D1:CE:7B:2D:EF:23:61:5B:3B:5A:EB:CA:CB:61:42:37:B7:47:CC:59:7B:40:1F:DA:5C:10:EB:15:81:0D:B6:3E:E3:AE:E4:3A:A7:A9:57:C7:79:05:C9:3C:2D:D1:97:54:40:34:BK:41:58:AK:0D:28:CD:87:9D:4B:B4:2C:43:5D:F4:42:87:99:D0:11:6E:F1:5A:59:D5:EC:20:AE:85:EF:10:79:A7:F7:06:F7:57:01:64:6F:DC:B6:D8:FF:6C:EA:BD:88:03:AA:FC:8E:2F:E9:7A:A3:17:07:2E:BE:AD:9B:77:31:18:01:51:79:F7:38:F9:71:3D:43:6D:D1:15:C1:52:BF:A2:A1:8F:83:FE:5B:87:E3:24:B7:A5:AF:BD:C0:DD:5C:35:52:B6:6A:3E:89:44:46:1D:CF:E7:DA:96:29:09:48:5C:FB:20:86:E8:46:F7:CB:D9:D4:16:CC:52:A6:7A:FE:D6:77:AD:E9:0A:C2:4C:48:17:D1:89:81:94:20:4B:03:08:08:1F:FC:37:85:B5:BF:06:AF:D5:05:DA:B3:4C:C5:BB:B0:76:90:6F:13:18:6A:CB:91:78:55:5E:4B:2C:6D:E0:C1:54:AB:70:07:C9:47:71:D9:C6:95:62:37:68:9F:3D:D7:13:1A:F0:0C:AB:1B:D3:3C:5E:D4:FF:25:74:D5:33:1D:61:B4:D4:0F:35:CB:8C:73:C9:EA:69:F3:25:2E:7F:0D:4C:4B:F8:2A:E8:C2:C5:94:20:BB:6C:F6:3B:0F:E1:49:48:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *50:47:5C:2F:BA:12:7B:5F:74:38:1B:07:12:31:FB:68:4C:A8:EF:DE*

Authority Key Identifier *B5:2E:59:20:B2:AF:43:BB:95:3D:C2:51:99:E3:75:55:34:48:B0:1C*

Authority Info Access

http://www.camerfirma.com/certs/chambersofcommerceroot2018.crt

http://ocsp.camerfirma.com

Extended Key Usage *id_kp_serverAuth*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://policy.camerfirma.com

CRL Distribution Points

http://crl.camerfirma.com/chambersofcommerceroot2018.crl

http://crl1.camerfirma.com/chambersofcommerceroot2018.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BF:0F:44:91:F3:71:48:9D:F2:EB:18:7B:DC:B4:B2:ED:D9:AB:2D:A0:16:CC:64:08:4C:AC:45:19:5E:F3:59:0D*

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *UEdcL7oSe190OBsHEjH7aEyo794=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2020-04-28T00:00:00Z*

11.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

11.17.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES 2018*

Name [es] *Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES 2018*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*UEdcL7oSe190OBsHEjH7aEyo794=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2019-09-15T22:00:00Z*

11.17.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

12 - TSP: COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

.

TSP Name

Name	*[en]*	*COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA*
Name	*[es]*	*COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA*

TSP Trade Name

Name	*[en]*	*VATES-Q2863012G*
Name	*[en]*	*REGISTRADORES DE ESPAÑA*
Name	*[es]*	*REGISTRADORES DE ESPAÑA*
Name	*[en]*	*Colegio de Registradores de la Propiedad y Mercantiles de España*
Name	*[en]*	*Colegio de Registradores de la Propiedad y Mercantiles*

PostalAddress

Street Address	*[en]*	*C/Diego de León, 21*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28006*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*C/Diego de León, 21*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28006*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.registradores.org*
URI	*[en]*	*mailto:psc@registradores.org*

TSP Information URI

URI	*[en]*	*http://pki.registradores.org/normativa/en/tsp_information.htm*
URI	*[es]*	*http://www.registradores.org*

12.1 - Service (withdrawn): Qualified Certificate issued by internal CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificate issued by internal CA*
Name	*[es]*	*Certificado reconocido emitido por la CA certificados internos*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *753384515004732294990404759965765290 77*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHezCCBWOgAwIBAgIQQK2ocMceA09FwGl6G+u6tTANBgkqhkiG9w0BAQUFADCBpDELMAkGA1UE
BhMCRVMxSjBIBgNVBAoMQUNvbGVnaW8gZGUgLmVnaXN0cmFkb3JlcyBkZSBsYSfBQcm9waWVkYWQg
cSBNZXJfYW50aWxlcyBkZSBFc3Bhbw7FhMRswGQYDVQQLDBJDZXJ0aWZpY2FkbyBQcm9waW8xLDAq
BgNVBAMM1IJfZ1lzdHJhZG9yZXMgZGUgRXNwYcOxYSAtIENBIFJhw616MB4XDTA3MDEzMTEwMDMz
OFoXDTE5MDEzMTA4MzExMFowgaYxCzAJBgNVBAYTAkVTMUowSAYDVQQKDEFDb2xlZ2lvIGRlIFJI
Z2lzdHJhZG9yZXMgZGUgbGEgUHVvcGlvZGFkIHkgTWVyY2FudGlsZXMgZGUgRXNwYcOxYTEhMBkG
A1UECwwSQ2VvdGlmaWNhZG8gUHVvcGlvMS4wLAYDVQQDDCVSZWdpc3RyYWRvcmVzIGRlIEVzcGHD
sWEgLSBDQSBJbnRlcm5hMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxQmR2gPdcYG4
4D+CcXMvUL1qOqa3PNussggPDPIsrtuzfLdkrph7n30rhrkeLWU5p1l4heFb83RswML6hpwugEIB
bR1ARvMREFBDr7pH8v7xLIvghBNux13LfcP47Q/+CseMivYkiwKwgH076sj9WQgNgBKIqUNiMGT4
tI9JQ9T4h/ai9tBknzJWi7KU8KnqaxJgNLCb9ytGAiXeb9yM9WJ/smnW9Pa4ajYGuzm0ogitlu0
oST+U/6tr+lzY+gzplnl6r8nINvKzl8YOHlhPDmYYBtnAXOCv4Z5TGvPPyBzl5vLjhBZHFX4s7MiqpF
KuSFcmZJ0mn3h/Z9/NW5Ol91ewIDAQABo4ICozCCAp8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
A8EBAMCAQYwHQYDVR0OBBYEFI7wY3d0cCC+y5SEITEVKtkN5Z0LMIH3BgNVHSAEge8wgewwgekG
BFUdIAAwgeAwPAYIKwYBBQUHAgEWMGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlcy5vcmcvbm9ybWF0
aXZhL2luZGVvL mhibbTCBmwYIKwYBBQUHAgIwgZIagY9DZXJ0aWZpY2FkbyBzdWplaG8gYSBsYSBE
ZWNsYXJhY2nzbiBkZSBQcuFjdGljYXMgZGUgQ2VydGlmaWNhY2nzbiBkZWwgQ29sZWdpbyBkZSBS
ZWdpc3RyYWRvcmVzIGRlIGxhIFByb3BpZWRhZCB5IE1lcmNhbnRpbGVzIGRlIEVzcGHxYSAoqSAy
MDA2KTBVBggrBgEFBQcBAQRJMEcwRQYIKwYBBQUHMAKGOWh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jl
cy5vcmcvY2Vvdi0lmaWNhZO9zL2NhX3JhaXp6c2NvLmNvdDAfBgNVHSMEGDAWgBQbYdcs7dYYmRm
rOLkpPaiGRL25TCB6gYDVR0fBIHiMIHfMIHfMIHfoIHZoIHWh1odfHRwOi8vcGtpLnJlZ2lzdHJhZG9y
ZXMub3JnL2NybHMvYXJsX3Njci5jcmyGgaRsZGFwOi8vbGRhcC5yZWdpc3RyYWRvcmVzLm9yZy9D
Tj1DQSUyMEJBSVosT1U9Q0VSVEIGSUNBRE8lMjBQU k9QSU8sTz1DT0xFR0lPJTIwREU1MjBSRUdJ
U1RSQUlRPUkVTLEA9RVM/YXV0aG9yaXRSUmV2b2NhdGlvbkxpc3Q/YmFzZT9yYmplY3RjbGFzcz1j
UkxfaXN0kmldXRpb25Qb2luaDANBgkqhkiG9w0BAQUFAAOCAgEAqtIRNnLAyz5VjTVQPWS9B2AD
KtoV5N90sSMGl7tkY2qNQ8SCJF+lnRYYyk9IqdsI6vABKqBy0nzRWraD4Ta9a89UDqW8bx0SpuPP
bgt0lgk6ehRMSumLZgDNe48w6hKdRZhMAHZdSIf5I/dNnVG771zMSdgP/144afkdndj21AucA9zb
DEfTsYmmQB1DwJFqBjqQSSjMxum+zhvcOa90jksN8r1apGit264a6LF0OV6KsSg4byb dK/DTWLIM
xNvrda4XhbyaqQHqRg1VFyydMNaPTrIlIQgYYgC9b0NGa14C1Nu74AE39hmScregFiU/hjckddW
EuKgruhDD6aWhupjap+ONB/B6M59lpRB9SyONMC/PEeCVUwFhq2pQnhmrslssmEqJVmRyHBCpiTs
Z7539sDSAZos8ofbwK5tjhA2S5Okz063Dr0QvXUXWCC/2777Wi530i8GyE0ksxpHBpSHneZnk2z7
ACcvOV3mEqz49I4kMBSU/gdIiBJow68vYKPbT40Eg/10pBzQmnHXqxrxW3CrtIsDvSgar+tWrLE
cSYELOqQuB12IHt8fmSOmU0czfUSPDxylYgDtD1gXKLCT7prZplpuxbkocCWsVYIb3itkzGmjg
AiRCTYroUyW5Q1Z9T3tSbBxwJTWHhxAlc+vdLwY/yt2BNyj2wyI=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Registradores de España - CA Raíz*

Issuer OU: *Certificado Propio*

Issuer O:	*Colegio de Registradores de la Propiedad y Mercantiles de España*
Issuer C:	*ES*
Subject CN:	*Registradores de España - CA Interna*
Subject OU:	*Certificado Propio*
Subject O:	*Colegio de Registradores de la Propiedad y Mercantiles de España*
Subject C:	*ES*
Valid from:	*Wed Jan 31 11:03:38 CET 2007*
Valid to:	*Thu Jan 31 09:31:10 CET 2019*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:09:91:DE:03:DD:79:81:B8:E0:3F:82:71:73:2F:50:BD:6A:3A:A6:B7:3C:DB:AC:B2:C8:0F:0C:F2:2C:AE:DB:B3:7C:B7:64:AE:98:7B:9F:7D:2B:86:B9:1E:2D:65:39:A7:59:78:85:E1:5B:F3:74:6C:C0:C2:FA:86:9C:2E:80:49:41:6D:1D:40:46:F3:11:10:50:43:AF:BA:47:F2:FE:F1:2C:8B:E0:84:13:6E:C4:8D:CB:7D:C3:F8:ED:0F:FE:0A:C7:8C:8A:F6:24:8B:02:B0:80:7D:3B:EA:C8:FD:59:08:0D:80:12:88:A9:43:62:30:64:F8:B4:8F:49:43:D4:F8:87:F6:A2:F6:D0:64:9C:95:A2:EC:A5:3C:2A:7A:9A:C4:98:0D:2C:28:7D:B7:2B:46:02:25:DE:6F:DC:8C:F5:62:7F:B2:69:D6:F4:F6:B8:6A:58:D8:1A:EC:E6:3A:88:22:B6:5B:B4:A1:24:E2:E1:4E:AD:AF:E9:73:63:E8:19:A6:5E:AB:97:FF:27:1C:DB:CA:CE:5F:18:38:76:CF:0E:66:3B:06:70:17:38:28:B8:67:94:C6:BC:F3:F2:05:DE:6F:2E:38:41:64:71:57:E1:2E:CC:8A:AA:45:2A:E4:85:72:66:49:D2:69:F7:87:F6:7D:FC:D5:B9:3A:5F:75:7B:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*8E:F0:63:77:74:70:20:BE:CB:94:84:95:31:15:2A:D9:0D:E5:9D:0B*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://pki.registradores.org/normativa/index.htm* *CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2006)]*
Authority Info Access	*http://pki.registradores.org/certificados/ca_raiz_scr.crt*
Authority Key Identifier	*1B:8D:59:1C:B3:B7:58:62:64:66:AC:E2:E4:A4:F6:A2:19:12:F6:E5*
CRL Distribution Points	*http://pki.registradores.org/crls/arl_scr.crl* *ldap://ldap.registradores.org/CN=CA%20RAIZ,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*3A:50:ED:C2:11:47:D8:67:37:75:C7:07:D3:2F:19:7D:DC:BE:34:75:BF:07:41:50:31:9E:11:61:DD:77:19:59*

X509SubjectName

Subject CN:	*Registradores de España - CA Interna*
Subject OU:	*Certificado Propio*
Subject O:	*Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-02-06T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

12.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificate issued by internal CA*

Name *[es]* *Certificado reconocido emitido por la CA certificados internos*

Service digital identities

X509SubjectName

Subject CN: *Registradores de España - CA Interna*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

X509SKI

X509 SK I *jvBjd3RwIL7LlISVMRUq2Q3lnQs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

12.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificate issued by internal CA*

Name *[es]* *Certificado reconocido emitido por la CA certificados internos*

Service digital identities

X509SubjectName

Subject CN: *Registradores de España - CA Interna*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

X509SKI

X509 SK I *jvBjd3RwIL7LlISVMRUq2Q3lnQs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-02-13T00:00:00Z*

12.2 - Service (withdrawn): Qualified Certificate issued by external CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificate issued by external CA*

Name *[es]* *Certificado reconocido emitido por la CA certificados externos*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *168799944087747445566487799301312826182*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHezCCBWOgAwIBAgIQfv2vyxvrwRtFwGmjAqdLRjANBgkqhkiG9w0BAQUFADCBpDELMAkGA1UE
BhMCRVMxSjBIBgNVBAoMQUNvbGVnaW8gZGUgUmVnaXN0cmFkb3JlcyBkZSBsYSBQcm9waWVkYWQg
eSBNZXJjYW50aWxlcyBkZSBFc3Bhw7FhMRswGQYDVQQLDBJDZXJ0aWZpY2FkbyBQcm9waW8xLDAq
BgNVBAMM1UJlZ2lzdHJhZG9yZXMgZGUgRXNwYcOxYSAtENBIFJhw616MB4XDTA3MDEzMTEwMDQx
OVoXDTE5MDEzMTAxNTU3OFowgaYxCzAJBgNVBAYTAkVTMUowSAYDVQQKDEFDb2xlZ2lvIGRlIFJl
Z2lzdHJhZG9yZXMgZGUgbGEgUHJvcGllZGFkIHkgTWVyY2FudGlsZXMgZGUgRXNwYcOxYTEbMBkG
A1UECwwSQ2VydGlmaWNhZG8gUHJvcGlvMS4wLAYDVQQDDCVSZWdpc3RyYWRvcmVzIGRlIEVzcGHD
sWEgLSBDQSBFcHRlcm5hMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxfsR0TQLkoua
fLIFq7JXsDTncXLWoyDskcukvJvYyegzUXEFXvcwy92xM8tUcH7SnKvxggwyWywFcH5lkQOHZHb
UnYH5RM9SuQDYEB6THd7tZZrS6Vw0V1n6/51+h18hk17YzDdL1nplF6oFl962F1scCTsQRhqGEyZ
LPpdW0FtbaSfW0dR/LaD8SirXp16Q3diNwWr6MgoWbCG0qf3NUJWZIe9ykdQ8G/atxF+HhaJQcED
4Zvw84HqqTZF+JcEMqd05ogc+aObyAocxzxiTH/YyKD1DjclvI6fWM78426IVDHNmp4Ra5eFcU
wxfXI1b+rVrplAbHOeWhznKQIDAQABo4ICorCCAp8wDwYDVR0TAQH/BAUwAwEBzAOBgNVHQ8B
AI8EBAMCAQYwHQYDVR0OBBYEFHOKA/X0s2ORvEs1WOqitMZHNOUMlH3BgNVHSAEge8wgewwgekG
BFUdIAAwgeAwPAYIKwYBBQUHAgEWMGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlcy5vcmcvbm9ybWF0
aXZhL2luZGV4Lmh0bTCBnwYIKwYBBQUHAgIwgZIagY9DZXJ0aWZpY2FkbyBzdWpldG8gYSBsYSBE
ZWNsYXJhY2nzbiBkZSBQcuFjdGljYXMgZGUgQ2VydGlmaWNhY2nzbiBkZWwgQ29sZWdpbyBkZSBS
ZWdpc3RyYWRvcmVzIGRlIGxhIFByb3BpZWRhZCB5IE1lcmNhbnRpbGVzIGRlIEVzcGHxYSAoqSAy
MDA2KTBVBggrBgEFBQcBAQRJMEcwRQYIKwYBBQUHMAKGOWh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jl
cy5vcmcvY2VydGlmaWNhZG9zL2NhX3JhaXpfc2NyLmNydDAfBgNVHSMEGDAWgBQbjVkcs7dYYmRm
rOLkpPaiGRL25TCB6gYDVR0fBIHiMIHfMIHfMIHcoIHZoIHWh1odHRwOi8vcGtpLnJlZ2lzdHJhZG9y
ZXMub3lnL2NybHRlY2lzX3X3X3Rlc5cmVGgzKbZGFwOi8vcGtpLnJlZ2lzdHJhZG9yZXMgZGUgRXNwYcOxYzLmNyZy9D
Tj1DQSUyMFJBSVosT1U9Q0VSVEIGSUNBRE8lMjBQUk9QSU8sTz1DT0xFR0lPJTlwREUlMjBSRUdJ
U1RSQURPUkVTLEM9RVM/YXV0aG9yaXR5UmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RjbGFzcz1j
UksxEaXN0cmlkXRph25Qb2luaDANBgkqhkiG9w0BAQUFAAOCAgEAR1TZnun/31KNsd6yTvVOCMAoH
y4SU08dU/DtrwNslcVWpehbbHwJYo37ronlMu5nLc7oUsyZc6aDARczG4sdW1I5LdrLidnAYd2K40S
nacFHbYLaiaOS3Pb6jK2rIrp8e8cFCE07tns8/o8jFFxOWmrEF0cmhhsfC04AhMUibOcQpaktrIi
C0cRa8bYJz5PzDaTuXMNRASek5AtSv3LsC2URUERLnbnP1wbEv2dlsLotfe+BbWcs76geLfYXG72
zLCQPJatFaVvbNOQ9418hhXyowaIQPp8tY+5GVVz8Zbcm/F0+3V4UN5A+pK3PwvWKF7FzTHOTA2K
tYGwrP61JGvfEXzEtGGZ51oq1cHydNE3zznJB8cqIPNhLEiQ4Yczjk9yWcMOuZIHGs5jC7Ans4Wd
b/c4bhREaqJViYI5bDuN2lRoMtHzeCMXtC4FSOKaG/iRbf02MkmzaLrC7MGcQvGjZTYjkwCoJaz
ID+A1EA4e99X1R33YTCNRebiBd4mxdP/2UUDL6l+UpuOYYbm9sXenqBRRSKKP3q91sV2OcY5biaB
vjhn7OJeJFOdp1NKFGhRjPSCibDUCmWTIj/gA+MCIZqSN8I6mVjpREHVsgPKrq4OOeWiNQRKxSYE
OBcxcAXwIdpogEcbM5C2nnv/FrhaLxK8NHWZq2FL05c4qXI65vM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Registradores de España - CA Raíz*

Issuer OU: *Certificado Propio*

Issuer O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Issuer C: *ES*

Subject CN: *Registradores de España - CA Externa*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

Valid from: *Wed Jan 31 11:04:19 CET 2007*

Valid to: *Thu Jan 31 09:55:28 CET 2019*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B1:FB:11:D1:34:0B:92:8B:9A:7C:B9:45:AB:B2:57:C4:34:E7:71:72:D6:A3:20:EC:91:CB:A4:BC:9C:98:8D:E8:22:CD
:45:C4:15:7B:DC:C3:2F:76:C4:CF:2D:51:C1:FB:4A:72:AF:C6:08:30:8D:68:F0:15:C1:F9:96:44:0E:1D:91:E1:52:76:07:E5:13:3D:4A:E4:03:60:40:7A:4C:77:7B:B5:96:6B:4B:A5:70:D1:5D:67:EB:FE:75:FA:1D:7C:86:49:7B:6
3:30:DD:2F:59:E9:94:5E:A8:16:5F:7A:D8:5D:6C:70:24:EC:41:18:6A:18:4C:99:2C:FA:5D:5B:41:6D:6D:A4:9F:5B:47:51:FC:B6:83:F1:28:AB:5E:9D:7A:43:77:62:37:05:AB:E8:C8:28:5A:10:86:D2:A7:F7:35:42:56:64:87:BD
:CA:47:50:F0:6F:DA:B7:11:7E:1E:16:89:41:C1:03:E1:9B:F0:F3:81:EA:A9:36:45:F8:97:04:33:FA:9D:D3:9A:20:73:E6:8E:6F:20:28:73:1C:F1:8A:24:C7:FD:8C:8A:0F:50:E3:72:5B:C8:E9:F5:8C:EF:CE:36:EA:55:43:1C:D9:A
9:E1:16:B9:78:57:14:C3:17:C9:5C:8D:61:FA:B5:63:A4:80:1B:1C:E7:96:6E:29:CA:89:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier	*73:8A:03:F5:F4:B3:63:91:BC:4B:35:58:EA:A2:89:F3:19:1C:D3:94*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://pki.registradores.org/normativa/index.htm* *CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2006)]*
Authority Info Access	*http://pki.registradores.org/certificados/ca_raiz_scr.crt*
Authority Key Identifier	*1B:8D:59:1C:B3:B7:58:62:64:66:AC:E2:E4:A4:F6:A2:19:12:F6:E5*
CRL Distribution Points	*http://pki.registradores.org/crls/arl_scr.crl* *ldap://ldap.registradores.org/CN=CA%20RAIZ,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*13:51:F3:92:83:7A:73:9D:D8:53:D7:F8:E2:FE:FF:39:12:77:18:79:82:1F:A4:76:14:DB:87:A3:AF:03:5C:E6*

X509SubjectName

Subject CN:	*Registradores de España - CA Externa*
Subject OU:	*Certificado Propio*
Subject O:	*Colegio de Registradores de la Propiedad y Mercantiles de España*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-02-06T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

12.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

12.2.2 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificate issued by external CA

Name [es] Certificado reconocido emitido por la CA certificados externos

Service digital identities

X509SubjectName

Subject CN: Registradores de España - CA Externa

Subject OU: Certificado Propio

Subject O: Colegio de Registradores de la Propiedad y Mercantiles de España

Subject C: ES

X509SKI

X509 SK I c4oD9fSzY5G8SzVY6qKJ8xkc05Q=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

12.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

12.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificate issued by external CA

Name [es] Certificado reconocido emitido por la CA certificados externos

Service digital identities

X509SubjectName

Subject CN:	*Registradores de España - CA Externa*
Subject OU:	*Certificado Propio*
Subject O:	*Colegio de Registradores de la Propiedad y Mercantiles de España*
Subject C:	*ES*

X509SKI

X509 SK I	*c4oD9fSzY5G8SzVY6qKJ8xkc05Q=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2009-02-13T00:00:00Z*

12.3 - Service (granted): Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Interna

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Interna*
Name	*[es]*	*Certificados cualificados emitidos por Autoridad de Certificación de los Registradores - AC Interna*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*332501078835806133010757615664522522 03*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIkzCCBnugAwIBAgIQGQO840KCd2BXVYr56bd+KzANBgkqhkiG9w0BAQ0FADCBqTELMAkGA1UE
BhMCRVMxGDAWBgNVBGEMD1ZBVEYTLVEyODYzMDEyRzEMD0GA1UECgw2Q29sZWdpbyBkZSBSZWdp
c3RyYWRvcmVzIGRlZGxhIFByb3BpZWRhZCBSIEIlcmNhbnRpbGVzMTIwPQYDVQQDDDZBdXRvcmlk
YWQgZGUgQ2VydGlmaWNhY2nDs24gUmHDrXogZGUgbG9zIFJlZ2ludHJhZG9yZXMwHhcNMTYwNjA2
MTQzODQ4WhcNMjgwNjA2MTQzODQ4WjCBsDELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLVEy
ODYzMDEyRzE3MD0GA1UECgw2Q29sZWdpbyBkZSBSZWdpc3RyYWRvcmVzIGRlIGxhIFByb3BpZWRh
ZCBSIEIlcmNhbnRpbGVzMUYwRAYDVQQDDD1BdXRvcmlkYWQgZGUgcG2VydGlmaWNhY2nDs24gZGUg
bG9zIFJlZ2ludHJhZG9yZXMgLSBBQyBJbnRlcm5hMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEAkwKMNvzIJasUpint0VoW4WfXHJv0MaSzvsI+VEfixf0eyx88F7LN4C6gMcsVsc9DchZg
1BGrp9qvWl4l2mLCn+WZwqTuDa2uWJsu5uEo7G85yahiEVwIGrsNuvv+IovEIwEWnghjmHCs38Ei
5QQ01I3sgrFyTMmXCsyJGsIlP9JeroshCjqsr635+JFf8AFwZqZ77w6HaBSRHaoi9HrXXIA5O0tc
ZLiewWOsf8rmg6PNl+bhCnQvPFrHyAWKJaZmFCUwovF6Q8XB5BWBfMMTd0JvA3i2J+DMIwdOQRvM
KA0/fKy56fDlAKozT18C07MH3dnDcv8tCj13JNcWtPUy10wjgSEW9N4f/e1R25yyzI6aB4S64xdS
L8TMl8ITJKC6O3PHTHxiW9N/wm8YUlU/fe5sP24m732ITghsxAazOq5u/LWR4jkPFOgdhPWYvNzv
istMcvDGvSAx54RUT2+k2Cr4nNBSRu66dfVv4KS5cBGBoumB7xxsMpXOysAk2vsTnLNfjSTRfDnT
lzDPbfoOmEvfimrCWT2aDA3qnjhKVIYVabz6YTxgA+Ux0ArQde6GMpfGPFQIye0jKgfilJGHnIHxy
nEtDThR1yifdawdY17giDGEqAlmcA+C17EWWxiScorREMV3+3FI8hRMfVGwIGkvItsl7XqzDBLEb
S4zeUu8CAwEAAaOCAqwwggKoMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0G
A1UdDgQWBBTYsFmhIAUSK26bF1co0xEBW6+BDTCB9wYDVR0gBIHvMIHsMIHpBgRVHSAAMIHgMDwG
CCsGAQUFBwIBFjBodHRwOi8vcGtpLnJlZ2ludHJhZG9yZXMub3JnL25vem1hdGl2YS9pbmRleC5o
dG0wgZ8GCCsGAQUFBwICMIGSGoGPQ2VydGlmaWNhZG8gc3VqZXRvIGEgbGEgRGVjbGFyYWNp824g
ZGUgUHLbY3RpY2FzIGRlIENlcnRpZmljYWNp824gZGVsIENvbGVnaW8gZGUgUmVnaXN0cmFkb3ll
cyBkZSBsYSBQcm9waWVkYWQgeSBNZXJjYW50aWxlcyBkZSBFc3BhbWEgKkkgMjAxNikwXAYIKwYB
BQUHAQEEUDBOMEwGCCsGAQUFBzAChkBodHRwOi8vcGtpLnJlZ2ludHJhZG9yZXMub3JnL2NlcnRp
ZmljYWRvcy9hY19yYWI6X3BzY19jb3JwbWUuY3J0MB8GA1UdIwQYMBaAFNpyOGFABpflAvFtadsE
AennDKPnMIHpBgNVHR8EgeEwgd4wgdugdiggdWGNGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlcy5v
cmcvY3Jscy9hcmxfcHNyX2NvcnBlZS5jcmyOgZXsZGFwOi8vbGRhcC5yZWdpc3RyYWRvcmVzLm9y
Zy9DTyIyMFJBSVosTz1Db2xlZ2lvJTIwZGUlMjBSZWdpc3RyYWRvcmVzITwLSUyMFEyODYz
MDEyRyxDPUVTP2F1dGhvcml0eVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlz
dHJpYnV0aW9uUG9pbnQwDQYJKoZIhvcNAQENBQADggIBAE0TC77ThtmmhZf9zh6dQU/B3IjZ8uMR
VEOKfvu8s3qL4abz4okk0/Q4QeAa8aaMmg2zMOmnrbsycG+BPeOg79snjqTCgipOSG+KCrMzHxJy
Nr+yTlGFvT1Foyym1mGvBvMtEZbJdl.56SVQuqbJMuk9SU/y8iqD2Pvy3qYcA8KBkS4XKVExGluE+
3uuFEmVs3jSpjmbBg3ZvgphFKocUh0imnbs13zj8QVp7bxY+tSeO8ChCfVlot1PtggeXIeEE6LQU
uUAuBJp9pwnanNZhesYNE4Cyc+aEaWs4EjGMqUc/Va1NwJ7L87Z0G8TtZ2pnSUJOq8s9QlOTkl+v
rrUXbYVHwtcbG7ScxJWYKpwg42Sq/axPh60aowm4yCWXRjaATm2umYt7mvtbFTJX3AI8pgTrMRm
zVzekqqoFWR2GIPCbWyQVOhFI3BWxAqz+qmnlRZg5w4Z2uX7mBbMLtwtLCCpiOCdWWQk9EjcxuBx
lGGE3cDs48bb5urXT9WXdN1bJwcbBwL3xX1oshNp4ed8eYR/tWnll2ChnN6eHg0kjHyQrt+uM2P
wnXOtlq+LggkJ5B30cVPMVJZgOQkQ3diRz2GvcVH3pt5Vee6X9983WIPqNm5kspXmwzvraEt+3Ya
BX9rFVu7YvhDr2inv/FJiR4mVnw9o8KmuvZIgir1iXpT

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: *Autoridad de Certificación Raíz de los Registradores*

Issuer O: *Colegio de Registradores de la Propiedad y Mercantiles*

Issuer 2.5.4.97: *VATES-Q2863012G*

Issuer C: *ES*

Subject CN: *Autoridad de Certificación de los Registradores - AC Interna*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

Valid from: *Mon Jun 06 16:38:48 CEST 2016*

Valid to: *Tue Jun 06 16:38:48 CEST 2028*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:93:02:8C:36:FC:E5:25:AB:14:A6:29:ED:D1:5A:16:E1:67:D7:1F:F2:6F:D0:C6:92:CE:FB:08:F9:51:21:C7:47:A3:C7:C
F:05:EC:B3:78:0B:A8:0C:72:C5:6C:73:D0:DC:87:96:60:D4:11:AB:A7:DA:AF:5A:52:78:DA:62:C2:9F:E5:59:C2:A4:EE:0D:AD:AE:58:9B:2E:E6:E1:28:EC:6F:39:C9:A8:62:11:5C:08:1A:BB:0D:BA:FB:FE:22:8B:C4:97:01:
16:36:08:63:98:70:AC:DF:C1:22:E5:04:25:D1:39:77:B2:9A:C5:C9:33:26:5C:2B:32:24:6B:08:94:FF:49:7A:BA:21:0A:AB:2B:EB:7E:7E:24:51:6D:F0:01:70:66:A6:7B:EF:0E:87:68:14:91:1D:AA:22:F4:1A:D7:5C:80:39:3B:48:
9E:64:B8:9E:C1:63:AC:7F:CA:E6:83:A3:CD:97:E6:E1:0A:74:2F:3C:5A:C7:C8:05:8A:25:A6:66:14:25:30:A2:F1:7A:43:C5:C1:E4:15:81:7C:C3:13:77:42:6F:03:78:B6:27:E0:CC:23:07:4E:41:1B:CC:28:0D:3F:7C:AC:B9:E9:F
0:C8:02:4A:33:4F:5F:02:D3:B3:07:DD:D9:C3:72:FF:2D:0A:3D:77:24:D7:16:B4:F5:32:23:4C:23:81:21:16:F4:DE:1F:FD:ED:51:DB:9C:B2:CC:8E:9A:07:84:BA:E3:17:52:2F:C4:CC:97:C2:13:24:A0:BA:3B:73:C7:4C:7C:62:5
B:D3:7F:C2:6F:18:50:85:1F:78:8B:0F:DB:89:BB:DF:69:53:12:08:6C:C4:06:B3:D2:AE:6E:FC:B5:91:E2:39:0F:15:08:1D:84:F5:9B:BC:DC:EF:8A:C3:9F:7B:FB:C3:1A:F4:80:B3:9E:11:51:4D:BE:93:60:AB:E2:73:41:49:1B:B
A:E9:DF:55:E0:A4:B9:70:11:81:A2:E9:C1:EE:FC:6C:32:95:CE:CA:C0:24:DA:F8:93:9C:B3:5F:8D:24:FC:7C:38:93:97:30:CF:6D:FA:0E:98:4B:DF:9A:B0:96:4F:66:83:03:7A:A7:8E:12:95:21:85:5A:6F:3E:98:4F:18:00:F9:4C
:74:02:B4:1D:7B:A1:8C:A5:F1:8F:15:02:32:7B:48:CA:81:F8:A5:24:61:E7:20:7C:72:9C:4B:43:4E:14:75:CA:27:DD:6B:07:58:D7:B8:23:0C:61:2A:02:59:9C:03:E0:B5:EC:45:96:C5:F4:9C:A2:B4:44:31:5D:FE:DC:57:FC:85:1
3:1F:54:6C:25:1A:4B:F5:B6:C9:7B:5E:AC:C3:04:B1:1B:4B:8C:DE:52:EF:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *D8:B0:59:A1:94:05:12:2B:6E:A1:17:57:28:D3:11:01:5B:AF:81:0D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://pki.registradores.org/normativa/index.htm

CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]

Authority Info Access *http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt*

Authority Key Identifier	*DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*
CRL Distribution Points	*http://pki.registradores.org/crls/arl_psc_corpme.crl* *ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F6:7A:0C:98:7D:0D:7D:5E:7E:CC:4A:69:FD:20:00:5E:D2:BD:50:3B:6D:CA:05:24:92:B2:D5:A3:ED:0B:B3:D8*

X509SubjectName

Subject CN:	*Autoridad de Certificación de los Registradores - AC Interna*
Subject O:	*Colegio de Registradores de la Propiedad y Mercantiles*
Subject 2.5.4.97:	*VATES-Q2863012G*
Subject C:	*ES*

X509SKI

X509 SK I	*2LBZoZQFEituoRdXKNMRAVuvgQ0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-02-22T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

12.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.4 - Service (granted): Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Externa

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Externa*

Name *[es]* *Certificados cualificados emitidos por Autoridad de Certificación de los Registradores - AC Externa*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *203966959070090462472052971660717727 56*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIkzCCBnugAwIBAgIQD1bCv/KRk0VXVZFkNFY2VDANBgkqhkiG9w0BAQ0FADCBqTELMAkGA1UE
BhMCRVMxGDAWBgNVBGEMD1ZBVEVTLVEyODYzMDEyRzE/MD0GA1UECgw2Q29sZWdpbyBkZSBSZWdp
c3RyYWRvcmVzIGRlIGxhIFByb3BpZWRhZCBSIE1lcmNhbnRpbGVzMTYwPQYDVQQDDDZBdXRvcmlk
YWQgZGUgQ2VydGlmaWNhY2nDs24gUmHDrXogZGUgbG9zIFJlZ2lzdHJhZG9yZXMwHhcNMTYwNjA2
MTUwNjExWhcNMjgwNjA2MTUwNjExWjCBsDEIMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLVEy
ODYzMDEyRzE/MD0GA1UECgw2Q29sZWdpbyBkZSBSZWdpc3RyYWRvcmVzIGRlIGxhIFByb3BpZWRh
ZCBSIE1lcmNhbnRpbGVzMUYwRAYDVQQDDD1BdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2nDs24gZGUg
bG9zIFJlZ2lzdHJhZG9yZXMgLSBBQyBFeHRlcm5hMlICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEAr6WNEsLll7jSZ+oFcLLUp47v5YLiBZjr889FgIJ91/jgpED7mSAss5IXwGgLqr3OC2V9L
t9HyHVHA2mTyZwesGePObFw3YG/fgMQhaLmaC0I7pEOTaws3aCH8UHhjm5U33PkNxC2Lw7fcC0LY
k1tuBINz27NfZRtRVIF8KYykK/obN9W6LBUnUOBGEALAHUyKvv1NHbWmFzgt06C3CSwkb6OlnVLXZr
PGxOSqcnPHbPzdJFqKPhbta T6MjdXJNSk0QNEIsJVbyf6j7tEgFqVÜU3hhEn9CrDA0ZwId+KPJ4M
m5x6YFZkt0sVh0C4nZ5wKi6QPrGac8brrVnqWmtDW/cnWjpwocp3ycR6Ftjc45VGlwdVfmJ6dFQA
hDMZiG3KAzX8KwEYnWBNlvWr9mlShxxMsz3ybFhiB1Z9F0xWCKSODDv8dPYGpLJN7TXDAwx2HUgR
xiKHHnemC9rVPdxhKPtQVQ5AG1YsMq3PF7eiYKNrM5JNsOMaoytcc2Buvcdeyj Lgcgvi NQ2v8Y3
EseHujkfEQajpFyqDXKoQt06mchHqTfeJwOppvx1ZGqr/BPWOVBHlolh3l6Xzi3Ik4Sy/IT7mQ19
VKdkHqgnOmqtK/XVdGL4qIby74QCE4PBxTOPcVpewGHHxgU4fES/Eh28aayA+t6X3/YTM1FVDhbz
+qazn6MCAwEAAaOCAqwwggKoMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0G
A1UdDgQWBBQ1uGXNNaCiD5qv4nX+2wxIUj0DQDCB9wYDVR0gB IHvMIHsMIHpBgRVHSAAMIHgMDwG
CCsGAQUFBwIBFjBodHRwOi8vcGtpLnIlZ2ladHJhZG9yZXMub3Jnl.25vcmlhdGl2YS9pbmRlcC5o
dG0wgZ8GCCsGAQUFBwICMIGSGoGPQ2VydGlmaWNhZG8gc3VqZXRvIGEgbGEgRGVjbGFyYWNp824g
ZGUgUHLbY3RpY2FzIGRIIENlcnRpZmljYWNp824gZGVsIENvbGVnaW8gZGUgUmVnaXN0cmFkb3Jl
cyBkZSBsYSBQcm9waWVkYWQgeSBNZXJjYW50aWxlcyBkZSBFc3Bh8WEgKkkgMjAxNikwXAYIKwYB
BQUHAQEEUDBOMEwGCCsGAQUFBzAChkBodHRwOi8vcGtpLnIlZ2ladHJhZG9yZXMub3Jnl.2NlcnRp
ZmljYWRvcy9hY19yYW16X3BzY19jb3JwbWUuY3J0MB8GA1UdIwQYMBaAFNpyOGFABpflAvFtadsE
AennDKPnMIHpBgNVHR8EgeEwgd4wgduggdiggdWGNGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlcy5v
cmcvY3Jscy9hcmxfcHNjX2NvcnBlZS5jcmyOgZXsZGFwOi8vbGRhcC5yZWdpc3RyYWRvcmVzLm9y
Zy9DTjIBQyUyMFJBSVosTzJDb2xlZ2lvJTIwZGUlMjBSZWdpc3RyYWRvcmVzITwLSUyMFEyODYz
MDEyRyxDPUVTP2F1dGhvcml0eVJldm9yYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlz
dHJpYnV0aW9uU/G9pbnQwDQYJKoZIhvcNAQENBQADggIBAKshh3HqHB6QJ3h2uxyvb4P3ZgsABwy0
12H/GM+AzkXB1vlhZxv21STFHbMNZSwtPBwEmwCBb9NWksub9u2ULqLOiIz/obK1ObCnfZ2555i
lcC3F1ZdX+f962cHvyLgVF8z2yEgvCOqEuxDIs9ozEre4SSydIMqgzwrE+vJpekkKnmCXtFvXf
hk5o7EH3kf501bVJ76F2soL58o4R94bNApEsG6Z/6Bm74dqSL8B99mNyQQvi6oSAGmFqD+PZOWJT
vPC/TaEau0RQghEWEI3Hxcv3D54Mfw4sthRBlp81GwFHqFuyF45kzZAjHYF+xc2rQbnwyQLhmMdj
7LaPa2t2EGLe07W17hkz2JhNiQit1mup3L0NVfSW6U/a20V0cait3Mn81zfmNVk9dH/ZTXQlZvYOG
A3gvyF0ZaT+TnwZvHMdSYbCthMR7IfjrI8fnc0jwnadbYzruYiHmNbfKcDkYSSHXWKOwVSLDzeN7q
WRtg4KorP6yDBw0ha0+KMjQ9rhBcxXUYWUMU+yoZH6WOx2bguNx13W9I3hqvGC1KJyg+Cjc5hH15
20A+vjgr8wk4xIcodecVffAvC4IQQJf4zeug5DRvx/4o1oD7ODQSUCxB7CF3IN6D+Fjte6O1kv3m
c38x8mXny55XbyRE0MJhnuSXi/90beLeE5Pant7IbZsB

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *Autoridad de Certificación Raíz de los Registradores*

Issuer O: *Colegio de Registradores de la Propiedad y Mercantiles*

Issuer 2.5.4.97: *VATES-Q2863012G*

Issuer C: *ES*

Subject CN: *Autoridad de Certificación de los Registradores - AC Externa*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

Valid from: *Mon Jun 06 17:06:11 CEST 2016*

Valid to: *Tue Jun 06 17:06:11 CEST 2028*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AF:A5:8D:12:C2:C8:97:B8:D2:67:EA:05:70:B2:D4:A7:8E:EF:E5:82:E2:05:98:EB:F3:CF:45:80:87:FD:D7:F8:E0:A4:40:FB:99:20:2C:E6:55:F0:1A:02:EA:AF:73:82:D9:5F:4B:B7:D1:F2:1D:51:C0:DA:64:F2:67:07:AC:19:E3:CE:6C:5C:37:60:6F:DF:80:C4:21:68:B9:9A:0B:4D:7B:A4:43:93:6B:0B:37:68:21:FC:50:78:63:9B:95:12:DC:F9:0D:C4:2D:8B:C3:B7:DC:0B:42:D8:93:5B:6E:04:83:73:DB:B3:45:65:18:95:20:5F:0A:63:22:8A:FE:88:4D:F5:6E:8B:05:49:D4:40:11:84:00:B0:07:53:22:AF:CB:53:47:6D:69:85:CE:0D:3A:0B:70:92:C2:46:FA:42:59:D5:2D:76:6B:3C:6C:4E:4A:A7:27:3C:76:CF:CD:D2:45:A8:A3:E1:6E:D6:93:E8:C8:DD:5C:93:52:93:44:0D:10:8B:09:55:BC:9F:EA:3E:ED:12:01:6A:55:45:37:86:11:27:F4:2A:C3:03:46:70:21:DF:8A:3C:9E:0C:9B:9C:7A:60:56:64:B7:4B:15:87:40:B8:9D:9E:70:2A:2E:90:3E:B1:9A:73:C6:EB:AD:59:EA:5A:67:C3:5B:F7:27:5A:3A:70:A1:CA:77:C9:C4:7A:16:D8:DC:E3:95:46:97:07:55:7E:62:7A:74:54:00:84:33:19:88:6D:CA:03:35:FC:2B:01:18:9D:60:4D:96:F5:A8:F6:69:52:86:BC:4C:B3:3D:F2:6C:58:62:07:56:7D:17:4C:56:08:A4:8E:0C:3B:FC:74:F6:06:A4:B2:4D:ED:35:C3:03:0C:76:1D:48:11:C6:D2:87:1E:77:A6:0B:DA:D5:3D:DC:61:28:F7:D0:55:0E:40:1B:56:2C:32:AD:CE:17:57:AE:60:A3:6B:33:92:5F:36:C3:8C:BA:88:F1:B5:ED:81:BB:27:1D:7B:28:CB:B6:07:20:BC:D4:36:BF:C6:37:12:C7:87:BA:39:1F:11:06:A3:A4:5C:AA:0D:72:A8:42:DD:3A:99:C8:47:A9:37:DE:27:03:A9:A6:FC:75:64:6A:AB:FC:13:D6:39:50:47:96:89:61:DE:5E:97:CE:2D:C8:93:84:B2:FC:8D:7B:99:0D:7D:54:A7:64:1E:A8:27:3A:6A:A2:2B:F5:D5:74:62:F8:A8:86:F2:EF:84:02:13:83:C1:C5:33:8F:79:5A:5E:C0:61:C7:C6:05:38:7C:44:BF:12:1D:BC:69:AC:80:FA:DE:97:DF:F6:13:33:51:55:0E:16:F3:FA:A6:B3:9F:A3:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *35:B8:65:CD:35:A0:A2:0F:9A:AF:E2:75:FE:DB:0C:48:52:3D:03:40*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://pki.registradores.org/normativa/index.htm

CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]

Authority Info Access *http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt*

Authority Key Identifier *DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*

CRL Distribution Points

http://pki.registradores.org/crls/arl_psc_corpme.crl

ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FB:7E:80:1D:60:D0:40:92:30:59:BD:31:CC:04:FA:49:C5:20:86:05:A0:09:C5:CB:D0:17:39:00:67:E6:57:17*

X509SubjectName

Subject CN: *Autoridad de Certificación de los Registradores - AC Externa*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

X509SKI

X509 SK I *NbhlzTWgog+ar+J1/tsMSFI9A0A=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2017-02-22T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

12.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.5 - Service (granted): Qualified timestamps issued by Autoridad de Certificación de los Registradores - TSA - 01

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified timestamps issued by Autoridad de Certificación de los Registradores - TSA - 01*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por Autoridad de Certificación de los Registradores - TSA - 01*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *215582907939921933829774971261693209 43*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIH3zCCBcegAwIBAgIQEDf5zKb6wodZQruotCGd7zANBgkqhkiG9w0BAQsFADCBsDELMAkGA1UE
BhMCRVMxGDAWBgNVBGEMD1ZBVEVTLVEyODYzMDEyRzE/MD0GA1UECgw2Q29sZWdpbyBkZSBSZWdp
c3RyYWRvcmVzIGRlIGxhIFByb3BpZWRhZCB5IE1lcmNhbnRpbGVzMUYwRAYDVQQDDD1BdXRvcmlk
YWQgZGUgQ2VydGlmaWNhY2nDs24gZGUgbG9yIFJlZ2IzdHJhZG9yZXMgLSBBQyBJbnRlcm5hMB4X
DTE3MDYxNTE2NTQwMFoXDTI4MDYwNjE0MzgzOCAJBgNVBAYTAkVTMRgwFgYDVQRhDA9W
QVRFUy1RMjg2MzAxMkcxPzA9BgNVBAoMNkNvbGVnaW8gZGUgUmVnaXN0cmFkb3JlcyBkZSBsYSBQ
cm9waWVkYWQgeSBNZXJjYW50aWxlczFEMEIGA1UEAww7QXV0b3JpZGFkIGRlIENlcnRpZmljYWNp
w7NuIGRlIGxvcyBSZWdpc3RyYWRvcmVzIC0gVFNBIC0gMDEwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDRIIr6KBIo9PSWjgwhEZDp+jouIgzTL Knos+r4dcKbZvKKat0jtRDIczRsK1b16C
E9JDcDYLe5WKOuuyKIgVg1vWAuUbEoS3c+/LHxw6ULGIHIE73jIVd2bHYGOzGSiKVlsmxJgTUkUZ
W77LzK7oxjRNAc024mtgHRcutWtO2uVlt6yPxR2LylHBTa2qd9+c8rXHpiktu3aAiSTVuUtrlLWv
nMKsxZp9DdxDzrWYJ89RuuD6+0ex3FUsKj/sz6i2icB/UoJRHFaYGT3qw36HqQPrIFxsAbE1t+u
YgrBmxxbHtuCwdSyqHSGdpJCrLoJ1oBRVxL7c/S0pMHdznumHEpAgMBAAGjggLzMIIC7zAOBgNV
HQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFMTIOUzVuv5EyhW1
tUss1IbrD/RpMIIBBAYDVR0gBIH8MIH5MIH2BgwrBgEEAYGGfAABCgEwgeUwPAYIKwYBBQUHAgEW
MGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlcy5vcmcvbm9ybWF0aXZhL2luZGV4Lmh0bTCBpAYIKwYB
BQUHAgIwgZcMgZRDZXJ0aWZpY2FkbyBzdWplk3BgYSBsYSBEZWNoYXJhY2nDs24gZGUgUHLDoWN0
aWNhcyBkZSBDZXJ0aWZpY2FjacOzbiBkZWwgQ29sZWdpbyBkZSBSZWdpc3RyYWRvcmVzIGRlIGxh
IFByb3BpZWRhZCB5IE1lcmNhbnRpbGVzIGRlIEVzcGHDsWEgKMKpIDIwMTYpMIGHBggrBgEFBQcB
AQR7MHkwKgYIKwYBBQUHMAGGHmh0dHA6Ly9YNwLnJlZ2lzdHJhZG9yZXMub3JnLzBLBggrBgEF
BQcwAoY/aHR0cDovL3BraS5yZWdpc3RyYWRvcmVzLm9yZy9jZXI0aWZpY2Fkb3MvYWNfaW5fX3Bz
Y19jb3JwbWUuY3JshoGhbGRhcDovL2xkYXAucmVnaXN0cmFkb3Jlcy5vcmcvQ049QUMlMjBJTlRF
Uk5BLE89Q29sZWdpbyUyMGRlITIwUmVnaXN0cmFkb3JlcyUyMC0lMjBRMjg2MzAxMkcsQz1FUz9j
ZXI0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2Jqa2Wh0Y2xhc3M9Y1JMRGlzdHJpYnVlaW9u
UG9pbnQwDQYJKoZIhvcNAQELBQADggIBAA1I+MiBXanzxb5SpPixytdC/TuBk7jNlXSjPwbrNE0f
GkMMfRWczRkqn6RqqxlA5HRjggkmxyEH48WBT+9RqUh0rTEC4d8g85Tx566TIrE5CsS8ITNhpuYG
9y7gFUyZV2JgU/dHUtOT49/oI+s4hiErnuM0uc T4Mxg3FDE6OimLUvWBzA5bgsOiJx/40jLXXVdS
7ogKWUBGKIryggJwL+xdt6QfUYYHdowWDH3PAPnwxUEW0mg2vkrIytOS9rT8U/BGRCCJGZ2H7kTm4
5g9IoxyHn5X89VdSvEcnzZxspmRGstvmkq9b8AfCq9uufiUJhMhmbWjdbFpMHHgBkyZVEECzhr25
xd/UtP20eJ4ndXpFS7GZ2tZNRtHnIVx8rKs112PT9PWs0A8Lyv2nL2RK9bO2/WM4K+sKnmBThSZs
JNYiL1MYgI0JOP37HBJ0SqXEdiAAq7R4+12BgCgk91DkaNE1LJAHbrcthU899VGU5R6Xp1fyZp8C
0Ym7U9HF1DqmAtSRZEwIZkR95nrtE6DMqpBGTJqYrwNXHdk52vdeOrzFacNgRp+KM78o+BOcX9g
b3YPZnvkA5rC7dxjphgOZVDMv09fiFrCjdBEwiWGZvu/pqkrhqNo3vmk02jRcL1ZlawhOp3mL0eG
byj9q9VOX9Dpz1KYUYZxkAHM471OoVi

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN:	*Autoridad de Certificación de los Registradores - AC Interna*
Issuer O:	*Colegio de Registradores de la Propiedad y Mercantiles*
Issuer 2.5.4.97:	*VATES-Q2863012G*
Issuer C:	*ES*
Subject CN:	*Autoridad de Certificación de los Registradores - TSA - 01*
Subject O:	*Colegio de Registradores de la Propiedad y Mercantiles*
Subject 2.5.4.97:	*VATES-Q2863012G*
Subject C:	*ES*
Valid from:	*Thu Jun 15 18:54:00 CEST 2017*
Valid to:	*Tue Jun 06 16:38:48 CEST 2028*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D1:20:7A:FA:28:12:27:F4:FF:16:8E:0C:21:11:90:E9:FA:3A:2E:D6:08:93:2D:19:E8:B3:EA:F8:75:C2:9B:66:F2:8A:6B:48:ED:44:31:1E:46:C2:87:E9:3E:82:13:D2:43:70:36:0B:7B:95:8A:3A:EB:B2:28:88:15:83:5B:D6:02:E5:1B:12:84:B7:7B:EF:CB:1F:1C:3A:50:B1:88:1C:81:3B:DE:32:15:77:66:C7:60:63:B3:19:28:8A:56:DB:26:C4:98:13:52:45:19:5B:BE:CB:CC:AE:E8:C6:34:4D:01:CD:36:E2:6B:60:1D:17:AE:B5:6B:4E:DA:E5:65:B7:AC:8F:C5:1D:8B:CA:51:C1:4D:AD:A0:77:DF:9C:F2:B5:C7:A6:29:2D:BB:76:80:89:24:D5:B8:9B:6B:94:B5:AF:9C:C2:AC:C5:9A:7D:0D:DC:43:CE:D5:98:27:CF:51:BA:E0:FA:FB:47:B1:DC:55:2C:F2:48:FF:B3:3E:A2:DA:27:01:FD:4A:09:44:71:5A:60:64:F7:AB:0D:FA:1E:A4:0F:AF:51:6C:C4:08:44:22:DF:AE:62:0A:C1:9B:1C:5B:46:1B:42:C1:D4:B2:A8:74:86:76:91:02:AC:BA:09:D6:80:51:57:12:FB:73:F4:8E:A4:C1:DD:CE:7A:EE:98:71:29:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*C4:C8:39:4C:D5:BA:FE:44:CA:15:B5:B5:4B:2C:D4:86:EB:0F:F4:69*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.17276.0.1.10.1* *CPS pointer: http://pki.registradores.org/normativa/index.htm* *CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]*
Authority Info Access	*http://ocsp.registradores.org/* *http://pki.registradores.org/certificados/ac_int_psc_corpme.crt*
Authority Key Identifier	*D8:B0:59:A1:94:05:12:2B:6E:A1:17:57:28:D3:11:01:5B:AF:81:0D*
CRL Distribution Points	*http://pki.registradores.org/crls/crl_int_psc_corpme.crl* *ldap://ldap.registradores.org/CN=AC%20INTERNA,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*33:5A:CB:56:33:A7:34:AB:EA:D2:34:93:AD:91:0E:FC:C9:D7:EB:C3:43:06:E1:E4:8C:7B:AF:07:0C:11:2D:57*

X509SubjectName

Subject CN:	*Autoridad de Certificación de los Registradores - TSA - 01*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

X509SKI

X509 SK I *xMg5TNW6/kTKFbW1SyzUhusP9Gk=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2018-02-06T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

12.6 - Service (granted): OCSP Responses issued by Autoridad de Certificación de los Registradores - VA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

[es] *A los servicios de estado de validez del certificado que expidan Protocolo de estado de certificados en línea (OCSP) firmaron respuestas y el funcionamiento de un servidor OCSP como parte de un servicio de un proveedor de servicios de confianza que expiden certificados reconocidos.*

Service Name

Name *[en]* *OCSP Responses issued by Autoridad de Certificación de los Registradores - VA*

Name *[es]* *Respuestas OCSP emitidas por Autoridad de Certificación de los Registradores – VA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *332501078835806133010757615664522522 03*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIkzCCBnugAwIBAgIQGQO840KCd2BXVYr56bd+KzANBgkqhkiG9w0BAQ0FADCBqTELMAkGA1UE
BhMCRVMxGDAWBgNVBGEMD1ZBVEYTTVEyODYzMDEyRzEyMD0GA1UECgw2Q29sZWdpbyBkZSBSZWdp
c3RyYWRvcmVzIGRlIGxhIFByb3BpZWRhZCBSIEIlcmNhbnRpbGVzMTIwPQYDVQQDDDZBdXRvcmlk
YWQgZGUgQ2VydGlmaWNhY2nDs24gUmHDrXogZGUgbG9zIFJlZ2ludHJhZG9yZXMwHhcNMTYwNjA2
MTQzODQ4WhcNMjgwNjA2MTQzODQ4WjCBsDELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLVEy
ODYzMDEyRzE3MD0GA1UECgw2Q29sZWdpbyBkZSBSZWdpc3RyYWRvcmVzIGRlIGxhIFByb3BpZWRh
ZCBSIEIlcmNhbnRpbGVzMUYwRAYDVQQDDD1BdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2nDs24gZGUg
bG9zIFJlZ2ludHJhZG9yZXMgLSBBQyBJbnRlcm5hMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEAkwKMNvzIJasUpint0VoW4WfXHJv0MaSzvsI+VEfixf0eyx88F7LN4C6gMcsVsc9DchZg
1BGrp9qvWl4l2mLCn+WZwqTuDa2uWJsu5uEo7G85yahiEVwIGrsNuvv+IovEIwEWnghjmHCs38Ei
5QQ01I3sprFyTMmXCsyJGsIlP9JcrohCjqsr635+JFf8AFwZqZ77w6HaBSRHaoi9HtrXXIA5O0tc
ZLiewWOsf8rmg6PNl+hbCnQvPFrHyAWKJaZmFCUwovF6Q8XB5BWBfMMTd0JvA3i2J+DMIwdOQRvM
KA0/fKy56fDlAKozT18C07MH3dnDcv8tCj13JNcWtPUy10wjgSEW9N4f/e1R25yyzI6aB4S64xdS
L8TMl8ITJKC6O3PHTHxiW9N/wm8YUlU/fe5sP24m732ITghsxAazOq5u/LWR4jkPFOgdhPWYvNzv
istMcvDGvSAx54RUT2+k2Cr4nNBSRu66dfVv4KS5cBGBoumB7xxsMpXOysAk2vsTnLNfjSTRfDnT
lzDPbfoOmEvfimrCWT2aDA3qnjhKVIYVabz6YTxgA+Ux0ArQde6GMpfGPFQIye0jKgfilJGHnIHxy
nEtDThR1yifdawdY17giDGEqAlmcA+C17EWWxiScorREMV3+3FfhRMfVGwIGkvItsl7XqzDBLEb
S4zeUu8CAwEAAaOCAqwwggKoMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0G
A1UdDgQWBBTYsFmhIAUSKz6bF1co0xEBW6+BDTCB9wYDVR0gBIHvMIHsMIHpBgRVHSAAMIHgMDwG
CCsGAQUFBwIBFjBodHRwOi8vcGtpLnJlZ2ludHJhZG9yZXMub3JnL25vem1hdGl2YS9pbmRlcC5o
dG0wgZ8GCCsGAQUFBwICMIGSGoGPQ2VydGlmaWNhZG8gc3VqZXRvIGEgbGEgRGVjbGFyYWNp824g
ZGUgUHLbY3RpY2FzIGRlIENlcnRpZmljYWNp824gZGVsIENvbGVnaW8gZGUgUmVnaXN0cmFkb3ll
cyBkZSBzYSBQcm9waWVkYWQgeSBNZXJjYW50aWxlcyBkZSBFc3BhbWEgKkkgMjAxNiKwXAYIKwYB
BQUHAQEEUDBOMEwGCCsGAQUFBzAChkBodHRwOi8vcGtpLnJlZ2ludHJhZG9yZXMub3JnL2NlcnRp
ZmljYWRvcy9hY19yYWl6X3BzY19jb3JwbWUuY3J0MB8GA1UdIwQYMBaAFNpyOGFABpflAvFtadsE
AennDKPnMIHpBgNVHR8EgeEwgd4wgduggdiggdWGNGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlcy5v
cmcvY3Jscy9hcmxfcHNyX2NvcnBlZS5jcmyOgZXsZGFwOi8vbGRhcC5yZWdpc3RyYWRvcmVzLm9y
Zy9DTj1BQuUyMFJBSVosTz1Db2xlZ2lvJTIwZGUlMjRSZWdpc3RyYWRvcmVzITIwLSUyMFEyODYz
MDEyRyxDPUVTP2F1dGhvcml0eVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlz
dHJpYnV0aW9uUG9pbnQwDQYJKoZIhvcNAQENBQADggIBAE0TC77ThtmmhZf9zh6dQU/B3IjZ8uMR
VEOKfvu8s3qL4abz4okk0/Q4QeAa8aaMmg2zMOmnrbsycG+BPeOg79snjqTCgipOSG+KCrMzHxJy
Nr+yTlGFvT1Foyym1mGvBvMtEZbJdl.56SVQuqbJMuk9SU/y8iqD2Pvy3qYcA8KBkS4XKVExGluE+
3uuFEmVs3jSpjmbBg3ZvgphFKocUh0imnbs13zj8QVp7bxY+tSeO8ChCfVlot1PtggeXIeEE6LQU
uUAuBJp9pwnanNZhesYNE4Cyc+aEaWs4EjGMqUc/Va1NwJ7L87Z0G8TtZ2pnSUJOq8s9QlOTkl+v
rrUXbYVHwtcbG7ScxJWYKpwg42Sq/axPh60aowm4yCWXRjaATm2umYt7mvtbFTJX3AI8pgTrMRm
zVzekqqoFWR2GlPCbWyQVOHf3BWxAqz+qmnlRZg5w4Z2uX7mBbMLtwtLCCpiOCdWWQk9EjcxuBx
lGGE3cDs48bb5urXT9WXdN1bJwcbBwL3xX1oshNlp4ed8eYRrlWnll2ChnN6eHg0kjHyQrt+uM2P
wnXOtlq+LggkJ5B30cVPMVJZgOQkQ3diRz2GvcVH3pt5Vee6X9983WIPqNm5kspXmwzvraEt+3Ya
BX9rFVu7YvhDr2inv/FJiR4mVnw9o8KmuvZIgir1iXpT

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: *Autoridad de Certificación Raíz de los Registradores*

Issuer O: *Colegio de Registradores de la Propiedad y Mercantiles*

Issuer 2.5.4.97: *VATES-Q2863012G*

Issuer C: *ES*

Subject CN: *Autoridad de Certificación de los Registradores - AC Interna*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

Valid from: *Mon Jun 06 16:38:48 CEST 2016*

Valid to: *Tue Jun 06 16:38:48 CEST 2028*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:93:02:8C:36:FC:E5:25:AB:14:A6:29:ED:D1:5A:16:E1:67:D7:1F:F2:6F:D0:C6:92:CE:FB:08:F9:51:21:C7:47:A3:C7:C
F:05:EC:B3:78:0B:A8:0C:72:C5:6C:73:D0:DC:87:96:60:D4:11:AB:A7:DA:AF:5A:52:78:DA:62:C2:9F:E5:59:C2:A4:EE:0D:AD:AE:58:9B:2E:E6:E1:28:EC:6F:39:C9:A8:62:11:5C:08:1A:BB:0D:BA:FB:FE:22:8B:C4:97:01:
16:36:08:63:98:70:AC:DF:C1:22:E5:04:25:D1:39:77:B2:9A:C5:C9:33:26:5C:2B:32:24:6B:08:94:FF:49:7A:BA:21:0A:AB:2B:EB:7E:7E:24:51:6D:F0:01:70:66:A6:7B:EF:0E:87:68:14:91:1D:AA:22:F4:1A:D7:5C:80:39:3B:48:
9E:64:B8:9E:C1:63:AC:7F:CA:E6:83:A3:CD:97:E6:E1:0A:74:2F:3C:5A:C7:C8:05:8A:25:A6:66:14:25:30:A2:F1:7A:43:C5:C1:E4:15:81:7C:C3:13:77:42:6F:03:78:B6:27:E0:CC:23:07:4E:41:1B:CC:28:0D:3F:7C:AC:B9:E9:F
0:C8:02:4A:33:4F:5F:02:D3:B3:07:DD:D9:C3:72:FF:2D:0A:3D:77:24:D7:16:B4:F5:32:23:4C:23:81:21:16:F4:DE:1F:FD:ED:51:DB:9C:B2:CC:8E:9A:07:84:BA:E3:17:52:2F:C4:CC:97:C2:13:24:A0:BA:3B:73:C7:4C:7C:62:5
B:D3:7F:C2:6F:18:50:85:1F:78:8B:0F:DB:89:BB:DF:69:53:12:08:6C:C4:06:B3:D2:AE:6E:FC:B5:91:E2:39:0F:15:08:1D:84:F5:9B:BC:DC:EF:8A:C3:9F:7B:FB:C3:1A:F4:80:B3:9E:11:51:4D:BE:93:60:AB:E2:73:41:49:1B:B
A:E9:DF:55:E0:A4:B9:70:11:81:A2:E9:C1:EE:FC:6C:32:95:CE:CA:C0:24:DA:F8:93:9C:B3:5F:8D:24:FC:7C:38:93:97:30:CF:6D:FA:0E:98:4B:DF:9A:B0:96:4F:66:83:03:7A:A7:8E:12:95:21:85:5A:6F:3E:98:4F:18:00:F9:4C
:74:02:B4:1D:7B:A1:8C:A5:F1:8F:15:02:32:7B:48:CA:81:F8:A5:24:61:E7:20:7C:72:9C:4B:43:4E:14:75:CA:27:DD:6B:07:58:D7:B8:23:0C:61:2A:02:59:9C:03:E0:B5:EC:45:96:C5:F4:9C:A2:B4:44:31:5D:FE:DC:57:FC:85:1
3:1F:54:6C:25:1A:4B:F5:B6:C9:7B:5E:AC:C3:04:B1:1B:4B:8C:DE:52:EF:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *D8:B0:59:A1:94:05:12:2B:6E:A1:17:57:28:D3:11:01:5B:AF:81:0D*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://pki.registradores.org/normativa/index.htm

CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]

Authority Info Access *http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt*

Authority Key Identifier	*DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*
CRL Distribution Points	*http://pki.registradores.org/crls/arl_psc_corpme.crl* *ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F6:7A:0C:98:7D:0D:7D:5E:7E:CC:4A:69:FD:20:00:5E:D2:BD:50:3B:6D:CA:05:24:92:B2:D5:A3:ED:0B:B3:D8*

X509SubjectName

Subject CN:	*Autoridad de Certificación de los Registradores - AC Interna*
Subject O:	*Colegio de Registradores de la Propiedad y Mercantiles*
Subject 2.5.4.97:	*VATES-Q2863012G*
Subject C:	*ES*

X509SKI

X509 SK I	*2LBZoZQFEituoRdXKNMRAVuvgQ0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-02-06T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*
URI	*[en]*	*http://pki.registradores.org/certificados/ac_va_psc_corpme.crt*
URI	*[es]*	*http://pki.registradores.org/certificados/ac_va_psc_corpme.crt*

12.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13 - TSP: Banco Español de Crédito, S.A

.

TSP Name

Name	*[en]*	*Banco Español de Crédito, S.A*
Name	*[es]*	*Banco Español de Crédito, S.A*

TSP Trade Name

Name	*[en]*	*VATES-A28000032*
Name	*[en]*	*Banesto CA*
Name	*[es]*	*Banesto CA*
Name	*[en]*	*Banesto S.A. - C.I.F. A28000032*
Name	*[es]*	*Banesto S.A. - C.I.F. A28000032*

PostalAddress

Street Address	*[es]*	*Avda. Gran Vía de Hortaleza, 3*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28043*
Country Name	*[es]*	*ES*

PostalAddress

Street Address	*[en]*	*Avda. Gran Vía de Hortaleza, 3*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28043*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[en]*	*http://ca.banesto.es*
URI	*[en]*	*mailto:correo@banesto.es*

TSP Information URI

URI	*[en]*	*http://ca.banesto.es*
URI	*[es]*	*http://ca.banesto.es*

13.1 - Service (withdrawn): Banesto Qualified Certificates of previous CA PSC Banesto Clientes

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Banesto Qualified Certificates of previous CA PSC Banesto Clientes*
Name	*[es]*	*Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *133541311365006312211899543605729653832*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIF7jCCBNagAwIBAgIQZHce/EjobIQ8keTNT+l0SDANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFUzEhMB8GA1UEBxMYTWVzZW5hIDgwIDI4MDMzIC0gTWFkcmlkMSgwJgYDVQQKEx9CYW5lc3Rv
IFMuQS4gLSBDLkkuRi4gQTI4MDAwMDMyMRkwFwYDVQQDExBQU0MgQmFuZXN0byBSb290MB4XDTAy
MDMxNTEyMTA1M1oXDTEyMDMxNDIzMDAwMFoweTELMAkGA1UEBhMCRVMxITAfBgNVBAcTGE1lc2Vu
YSA4MCAyODAzMyAtIE1hZHJpZDEoMCYGA1UEChMfQmFuZXN0byBTLkEuIC0gQy5JLkYuIEEyODAw
MDAzMjEzMBsGA1UEAxMUUFNDIEJhbmYzdG8uZXpzW50ZXMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCdYURFiRkHdNHSUArtsh9Q7Zod25MIiA3GqhddACBG+4mDVV6H1Q2u2nCXuyMb
QdRcreH01vRmvhvYhlYkvdxWlapp1HCTDLsxMJ6cY s6Pa9nCuzD3P2wXC8wYjkgHFpOb+SxAI6WS
oBK4jSxSajgG1HWkkgEHXTm0UNYX6PY1qjuzFg9KcvOaWekwcLbjrZh4+2FkIL5RQKuZ1HWdR3qg
kiV9H1tPYnylgoXa54kKm7vHOAuPzA+sqm9jbjuuQoGsAby9W1TqsdtudQ2zalt3IIwoQ3F7F1
r8puM2tKlMnYmGV0ttHCHB8ceM+4Q85Lkvl0lvZrBFtXc15sqzijAgMBAAGjggJ0MIICcDAYBgNV
HRIEETAPgQ1jYUBiYW5lc3RvLmVzMBgGA1UdEQQRMA+BDWNhQGJhbmVzdG8uZXMwDwYDVR0TAQH/
BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCNETGvtck7kcRsAO3Qj2TeQuwOlMIGu
BgNVHSMEgaYwgaOAFOo6fjoQVLsaVS4PEYOrpFBqK5uIoXmkdzB1MQswCQYDVQQGEwJFUzEhMB8G
A1UEBxMYTWVzZW5hIDgwIDI4MDMzIC0gTWFkcmlkMSgwJgYDVQQKEx9CYW5lc3RvIFMuQS4gLSBD
LkkuRi4gQTI4MDAwMDMyMRkwFwYDVQQDExBQU0MgQmFuZXN0byBSb290ghCdb1yZBWSicqTpkVkk
Z8Y4MIIBCQYDVR0gBIIBADCB/TCB+gYJKwYBBAHWRAEBMIHsMDEGCCsGAQUFBwIBFiVodHRwOi8v
Y2FuYmFuZXN0by5lcy9SZXBvc2l0b3Jpby9EUEMvMHG2BggrBgEFBQcCAjCBqRqBpkVzdGUgY2Vy
dGlmaWNhZG8gaGEgc2lkbyBlbWl0aWRvIHBvciBQU0MgQmFuZXN0byBSb290IHkgc2UgZW5jdWVu
dHJhHJlZ3VsYWRvIHBvciBsYXMgY29uZGljaW9uZXMgZ2VuZXJhbGVzIGRlZmluaWRhcyBlbiBz
dSBEZWNsYXJhY2lvbiBkZSBQcmFjdGljYXMgZGUgQ2VydGlmaWNhY2lvbi4wPAYDVR0fBDUwMzAx
oC+gLYYraHR0cDov L2NhLmJhbmYzdG8uZXMvQ1JML1BTQ1Jvb3RCYW5lc3Rv L mNybDANBgkqhkiG
9w0BAQUFAAOCAQEAJCessMAMhmSSHl007VOo3H/oc/UmSUr1QN9B/iLaaBGFJsJWwzB6wxBt+v/
UNatED9ObOtM4fH1utPicwqMTxKlpoQ7b+cRja0zVaAtNaIqIB/Bc/V7b6tLGRVJ0+vgGnq+AGP9
YEfjqep/13Xd3NpxlclM2F05O+eyohcG0cqA/W78SbZxcrfBEVsyhEpL EdbtpqJIs5EC7n0RmWJ3
47p5SS+7oDN9BxpqgNq8AyAJ55ZjAPPnFndPd4QSJh/7SaZpYYzXngIbl/m9H8aO8ls0/mYqGwad
bsvPtgSR+RHdIN0LCvHTG6wwsBNznKosHVrwnkW57/Ax+9sN9YXZA==

-----END CERTIFICATE-----

Signature algorithm:	*SHA1withRSA*
Issuer CN:	*PSC Banesto Root*
Issuer O:	*Banesto S.A. - C.I.F. A28000032*
Issuer L:	*Mesena 80 28033 - Madrid*
Issuer C:	*ES*
Subject CN:	*PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

Valid from: *Fri Mar 15 13:10:53 CET 2002*

Valid to: *Thu Mar 15 00:00:00 CET 2012*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9D:61:44:45:89:19:07:74:D1:D2:50:0A:ED:B2:1F:50:ED:9A:1D:DB:93:08:88:0D:C6:AA:17:5D:00:20:46:FB:89:83:55:5E:87:D5:0D:AE:DA:70:97:BB:23:1B:41:D4:5C:AD:E1:F4:D6:F4:66:BE:1B:D8:86:56:24:BD:DC:56:21:AA:69:D4:70:93:0C:BB:31:30:9E:9C:62:CE:8F:6B:D9:C2:BB:30:F7:3F:6C:17:0B:CC:18:8E:48:07:16:93:9B:F9:2C:40:23:A5:92:A0:12:B8:8D:2C:52:6A:38:06:D4:75:A4:92:01:07:5D:39:B4:2C:D6:17:E8:F6:35:AA:3B:B3:16:0F:4A:72:F3:9A:59:E9:30:70:B6:E3:AD:98:78:FB:61:64:20:BE:31:40:AB:99:D4:75:9D:47:7A:A0:92:55:7D:1F:5B:4F:62:7C:88:82:85:DA:E7:88:8A:9B:BB:C7:38:0B:8F:CC:0F:A2:AA:6F:5F:8D:B8:EE:B9:0A:06:B0:06:F2:F5:6D:53:AA:C7:6D:B9:D4:36:8B:36:A5:B7:72:48:C2:84:37:17:B1:75:AF:CA:6E:33:6B:4A:94:C9:D8:98:65:74:B6:D1:C2:1C:1F:1C:78:CF:B8:43:CE:4B:92:F2:34:22:F6:6B:04:5B:57:73:5E:6C:AB:38:A3:02:03:01:00:01

Issuer Alternative Name *ca@banesto.es*

Subject Alternative Name *ca@banesto.es*

Basic Constraints *IsCA: true*

Subject Key Identifier *23:44:4C:6B:ED:72:4E:E4:71:1B:00:3B:74:23:D9:37:90:BB:03:A5*

Authority Key Identifier *EA:3A:16:3A:10:54:BB:1A:55:2E:0F:11:83:AB:A4:50:6A:2B:9B:89*

Certificate Policies

Policy OID: 1.3.6.1.4.1.11076.1.1

CPS pointer: http://ca.banesto.es/Repositorio/DPC/

CPS text: [Este certificado ha sido emitido por PSC Banesto Root y se encuentra regulado por las condiciones generales definidas en su Declaracion de Practicas de Certificacion.]

CRL Distribution Points *http://ca.banesto.es/CRL/PSCRootBanesto.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *53:99:01:61:F9:3C:B7:9E:6E:75:13:06:74:A4:53:DE:7E:2D:22:C8:1B:51:10:40:68:8B:66:7E:3F:65:35:30*

X509SubjectName

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

13.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier *1.3.6.1.4.1.18838.1.1*

13.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.1.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Banesto Qualified Certificates of previous CA PSC Banesto Clientes*
Name	*[es]*	*Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior*

Service digital identities

X509SubjectName

Subject CN:	*PSC Banesto Clientes*
Subject O:	*Banesto S.A. - C.I.F. A28000032*
Subject L:	*Mesena 80 28033 - Madrid*
Subject C:	*ES*

X509SKI

X509 SK I *I0RMa+1yTuRxGwA7dCPZN5C7A6U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2013-05-23T22:00:00Z*

13.1.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier *1.3.6.1.4.1.18838.1.1*

13.1.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Banesto Qualified Certificates of previous CA PSC Banesto Clientes*

Name *[es]* *Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior*

Service digital identities

X509SubjectName

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

X509SKI

X509 SK I *I0RMa+1yTuRxGwA7dCPZN5C7A6U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2009-10-16T00:00:00Z*

13.1.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier	*1.3.6.1.4.1.18838.1.1*

13.1.5 - History instance n.3 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Banesto Qualified Certificates of previous CA PSC Banesto Clientes*
Name	*[es]*	*Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior*

Service digital identities

X509SubjectName

Subject CN:	*PSC Banesto Clientes*
Subject O:	*Banesto S.A. - C.I.F. A28000032*
Subject L:	*Mesena 80 28033 - Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*I0RMa+1yTuRxGwA7dCPZN5C7A6U=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2004-11-25T00:00:00Z*

13.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier	*1.3.6.1.4.1.18838.1.1*

13.2 - Service (withdrawn): Banesto Qualified Certificates of CA PSC Banesto Clientes

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en]	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Banesto Qualified Certificates of CA PSC Banesto Clientes*
Name	*[es]*	*Certificados Reconocidos de Banesto de CA PSC Banesto Clientes*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *178504100647072812269282137159059266 77*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHWzCCBUOgAwIBAgIQDW3dKkZ/TJxJLZosMx/WFTANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFUzEhMB8GCA1UEBxMYTWVzZW5hIDgwIDI4MDMzIC0gTWFkcmlkMSgwJgYDVQQKEx9CYW5lc3Rv
IFMuQS4gLSBDLkkuRi4gQTI4MDAwMDMyMRkwFwYDVQQDExBQU0MgQmFuZXN0byBSb290MB4XDTA4
MTEyNjE4NTAwMFoXDTMwMTIzMDIyNDk1OVowcTELMAkGA1UEBhMCRVMxITAfBgNVBAcTGE1lc2Vu
YSAhMCAyODAzMyAtIE1hZHJpZDEoMCYGA1UEChMfQmFuZXN0byBTLkEuIC0gQy5JLkYuIEsyODAw
MDAzMjEdMBsGA1UEAxMUUFNDIEJhbmVzdG8gQ2xpZW50ZXMwggIiMA0GCSqGSIb3DQEBAQUAA4IC
DwAwggIKAoICAQCsO5D0+zxM//hxcYbyCopdDOe9mljTARZBGPMZQFkhS+atl7UNTzQ/j11HB9IT
7sJxGcKT+sxhi0GKMsXyvH8CG46DGRC+mD39Eu1fQ3+UAVE22jm3TyfC7npltSPtsLdemwCC2OTM
+6NC3eXBKCCzYVkSxUyPWVHUWgLaGZd152VMlfMK+5cnHkDAtyOLO0MfUOFVO+FboUXM2+dRbEV
Mp88W/Sc81NXfq0uIZYbnKYDsD3omaYFubW1+UQIIDHG2BBbyRDR58L7Yqmm8+k2gOO+cw12VV8t
WbxisyST7ngOVI4ACsF3mZprujOvlL38FFTIpzQzMhARL5V+20or9sDZgXc4DlIPst8Bmb C6JCZ
EaMFu6FZ/wGwGRZZq5RIKrjvm6WelrMxc1IsU8VPGDDDcmBDfSD4VS4rlmaHuNl+F3HCw49DqbW6
xzCy0xJS4dhDLDByWkwCMXzWSEq9M27Wr9x4/1Q9GRV7HeM5XaE9rT/APJ+bZhFfC3nbdhWSgpGb
NHvvzz0U/mwBIxG/myLPUB+A95MsRtPubcMoFMfgWrnQXKd760j80KQSnMsBcqJKFOMHISWcAZSzcqe
IlxJQ2qYV3aDDtloxyyNb13mHJl7aD9ky56b2sFm3iQM6oN5FpwCOdH8E+Gv58QApXdYqaxEGTcX
3xs5yyz9GTQQ5wIDAQABo4IB4TCCAd0wGAYDVR0SBBEwD4ENY2FAYmFuZXN0byS1czAYBgNVHREE
ETAPgQ1jYUBiYW5lc3Rv LmVzMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0G
A1UdDgQWBBR7d8mQVac6NGWXFH2XPyLSAs4OrIDAfBgNVHSMEGDAWgBRaVSldy8eWYk81vKdPhovXU
TsTM8jCCAQMGA1UdIASB+zCB+DCB9QYEVR0gADCB7DAxBggrBgEFBQcCARYlaHR0cDovL2NhLmJh
bmVzdG8uZXMvUmVwb3NpdG9yaW8vRFBDLzCBtgYIKwYBBQUHAgIwgakagaZFc3RIlGNlcnRpZmlj
YWRvIGhhIHNpZG8gZW1pdGlkbyBwb3IgUFNDIEJhbmVzdG8gUm9vdCB5IHNlIGVuY3VlbnRyYSBv
ZWd1bGFkbyBwb3IgbGFzIGNvbmRpY2ltbmVyYWxcyBkZWZpbmlkYXMgZW4gc3I/gRGVj
bGFyYWNpb24gZGUgUHhY3RpY2FzIGRlIENlcnRpZmlj YWNpb24uMDwGA1UdHwQ1MDMwMaAvoC2G
K2h0dHA6Ly9jYS5iYW5lc3RvLmVzL0NSTC9QU0NSb290QmFuZXN0byc jcmwwDQYJKoZIhvcNAQEF
BQADggIBAF34bfdU3L6VUAxokcuGRqho0NqNm3uGNHUF5+Fb9jAQYYQ3JPduE TGAUAHY3+kZDE0I
ib7HUiSI0GOoNBYhe+UmBHvcuUzKcwB49/PyKbvTrfdZPbTmZrWCOYmeoPHFE473oMLIVKH+5w
rIg38Y11 7FYxi/5/REkGXts26jC4qfphTzHE5GWzL99Vm4D30cNPu/EfUlrErLbmxU/C57mu2r2f
8Bj3pscv8fRNFN9NsHBZ/bUHPlAvoYkpufWrviGeZJBtHBAQOAWmmFUOhOzyLtfRo2Q0T6aEM7CJ
b98ZFb4sVYnWUOqIEv6FUB4PLT9KRIkdJ/6XIimuY6wu4VJbM8IO2tfKCS07C6GVSLEJ8B9gBMx
QnDN5CqqwEptRq+thXiBcVCb3Go7O1xD1qIEmUe3gkxiMjq3KheQXxY+NTnn+KAlns6unwDvIF6
s7NC7LPfa4EnOx7kCkzW6csUgmOeDFI9hGXaN7YnfgzO1xcM05PoyXHvmXvX+kysKRfyr6m1jX
xzqKJGjqkf5AfZmLzDx6sh9CdEQk0sBoE2LvSo/4vxlDCxb6HBb9pxbBAnbZIL5yYAX/7ca5atnA
OkY9nMs8CqX7GdAllkAYt6YMnu8HlbSuZHYWRriLyaCt3osBoMf2J8yLVFMUS7C5GfpsN3nE32nL
BoDEEuLa

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *PSC Banesto Root*

Issuer O: *Banesto S.A. - C.I.F. A28000032*

Issuer L: *Mesena 80 28033 - Madrid*

Issuer C:	*ES*
Subject CN:	*PSC Banesto Clientes*
Subject O:	*Banesto S.A. - C.I.F. A28000032*
Subject L:	*Mesena 80 28033 - Madrid*
Subject C:	*ES*
Valid from:	*Wed Nov 26 19:50:00 CET 2008*
Valid to:	*Mon Dec 30 23:49:59 CET 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AC:3B:90:F4:FB:3C:4C:FF:F8:71:71:86:F2:0A:8A:5D:0C:E7:BD:9A:58:E3:4C:04:59:04:63:CC:65:01:64:85:2F:9A:B4:8E:D4:35:3C:D0:FE:3D:47:07:D2:13:EE:C2:71:19:E2:93:FA:CC:61:8B:41:8A:32:C5:F2:BC:7F:02:1B:8E:83:19:10:BE:98:3D:FD:12:ED:5F:43:7F:94:01:51:36:DA:39:B7:4F:27:C2:EE:7A:48:B5:23:ED:B0:B7:5E:9B:00:82:D8:E4:CC:FB:A3:42:DD:E5:C1:FC:A0:82:CD:85:64:4B:15:32:3D:65:47:51:68:0B:68:66:5D:D7:9D:95:32:52:0C:2B:EE:5C:9C:79:03:02:DC:8E:2C:ED:0C:7D:43:85:54:EF:85:6E:85:17:33:6F:9D:45:B1:15:32:9F:3C:5B:F4:9C:F3:53:57:7E:AD:2E:21:96:1B:9C:A6:03:B0:3D:E8:99:A6:05:B9:B5:B5:F9:44:1F:94:31:C6:D8:10:72:44:34:79:F0:BE:D8:AA:69:BC:FA:48:B6:80:E3:BE:73:0D:76:55:5F:2D:5A:5C:62:B3:24:93:EE:78:0E:57:5E:00:0A:C1:77:99:9A:6B:BA:33:AF:94:BD:FC:14:54:C8:A7:34:33:32:10:11:2F:95:7E:DB:4A:2B:F6:C0:D9:81:77:38:0E:57:CF:B2:DF:01:99:B0:BA:24:2B:39:11:A3:05:BB:A1:59:FF:01:B0:19:16:59:AB:94:48:2A:B8:EF:9B:A5:9E:96:B3:31:73:52:2C:53:C5:4F:18:30:C3:72:60:43:7F:90:F8:55:2E:2B:96:66:87:B8:D9:7E:17:71:C2:C3:8F:43:A9:B5:BA:C7:30:B2:D3:12:52:E1:D8:43:2C:30:72:5A:4C:02:31:7C:D6:48:4A:BD:33:6E:D6:AF:DC:78:FF:54:3D:19:15:7B:1D:E3:39:5D:A1:3D:AD:37:C0:3C:9F:9B:66:11:5F:0B:79:DB:76:15:92:82:91:9B:34:7B:EF:CF:3D:14:9B:00:48:C4:69:B2:2C:F5:01:F8:0F:79:32:C4:6D:3E:E8:5C:32:81:4C:96:05:A6:41:72:9D:EF:AD:23:F3:41:90:4A:78:8C:B0:17:2A:D4:A1:4E:30:74:96:70:06:6C:67:1A:9E:94:8C:49:43:6A:98:57:76:83:0E:D2:68:C7:2C:8D:6F:5D:E6:1C:99:7B:68:3F:64:CB:9E:9B:DA:C1:66:DE:24:0C:EA:83:79:16:9C:02:39:D1:FC:13:E1:AF:E7:C4:00:A5:77:58:A9:AC:44:19:37:17:DF:1B:39:CB:2C:FD:19:34:10:E7:02:03:01:00:01*
Issuer Alternative Name	*ca@banesto.es*
Subject Alternative Name	*ca@banesto.es*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*53:77:C9:90:55:A7:3A:34:65:97:14:7D:97:3E:F2:FC:02:2E:0E:AC*
Authority Key Identifier	*5A:BD:29:5D:C8:17:96:57:CD:6F:29:D3:E1:A2:F5:D4:4E:C4:CC:F2*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://ca.banesto.es/Repositorio/DPC/* *CPS text: [Este certificado ha sido emitido por PSC Banesto Root y se encuentra regulado por las condiciones generales definidas en su Declaracion de Practicas de Certificacion.]*
CRL Distribution Points	*http://ca.banesto.es/CRL/PSCRootBanesto.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*46:6C:9A:9D:76:A6:A4:04:68:F9:18:BE:BD:9D:9F:10:41:78:A7:60:03:78:45:94:FF:94:3B:F7:8D:73:29:B9*

X509SubjectName

Subject CN:	*PSC Banesto Clientes*
Subject O:	*Banesto S.A. - C.I.F. A28000032*
Subject L:	*Mesena 80 28033 - Madrid*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

13.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier *1.3.6.1.4.1.18838.1.1*

13.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.2.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Banesto Qualified Certificates of CA PSC Banesto Clientes*

Name *[es]* *Certificados Reconocidos de Banesto de CA PSC Banesto Clientes*

Service digital identities

X509SubjectName

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

X509SKI

X509 SK I *U3fJkFWnOjRllxR9lz7y/AIuDqw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2013-05-23T22:00:00Z*

13.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier *1.3.6.1.4.1.18838.1.1*

13.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Banesto Qualified Certificates of CA PSC Banesto Clientes*

Name *[es]* *Certificados Reconocidos de Banesto de CA PSC Banesto Clientes*

Service digital identities

X509SubjectName

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

X509SKI

X509 SK I *U3fJkFWnOjRllxR9lz7y/AIuDqw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-10-16T00:00:00Z*

13.2.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier *1.3.6.1.4.1.18838.1.1*

14 - TSP: EDICOM CAPITAL, S.L.

.

TSP Name

Name	*[en]*	*EDICOM CAPITAL, S.L.*
Name	*[es]*	*EDICOM CAPITAL, S.L.*

TSP Trade Name

Name	*[en]*	*VATES-B96490867*
Name	*[en]*	*EDICOM*
Name	*[es]*	*EDICOM*
Name	*[es]*	*INTERCAMBIO ELECTRONICO DE DATOS Y COMUNICACIONES SL*
Name	*[es]*	*EDICOM CAPITAL SL*

PostalAddress

Street Address	*[en]*	*Calle Charles Robert Darwin, número 8*
Locality	*[en]*	*Paterna*
State Or Province	*[en]*	*Valencia*
Postal Code	*[en]*	*46980*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Calle Charles Robert Darwin, número 8*
Locality	*[es]*	*Paterna*
State Or Province	*[es]*	*Valencia*
Postal Code	*[es]*	*46980*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:acedicom@edicomgroup.com*
URI	*[en]*	*http://acedicom.edicomgroup.com*

TSP Information URI

URI	*[en]*	*http://www.edicomgroup.com/en_ES/home.html*
URI	*[es]*	*http://www.edicomgroup.com/es_ES/home.html*

14.1 - Service (withdrawn): Qualified certificates issued by the AC ACEDICOM Root

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by the AC ACEDICOM Root*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA ACEDICOM Root*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7029493972724711941*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFrTCCA52gAwIBAgIIYY3HhjisBggUwDQYJKoZIhvcNAQEFBQAwRDEWMBQGA1UEAwwNQUNFREID
T00gUm9vdDEMMAoGA1UECwwDUEtJMQ8wDQYDVQQKDAZFREIDT00xCzAJBgNVBAYTAkVTMB4XDTA4
MDQxODE2MjQyMloXDTI4MDQxMzE2MjQyMlowRDEWMBQGA1UEAwwNQUNFREID T00gUm9vdDEMMAoG
A1UECwwDUEtJMQ8wDQYDVQQKDAZFREIDT00xCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEA/5KV4WgGdrQsvFhIyv2AVClVYy1/kGWbEHV7w2rbYgIB8hiGtXxaOLHk
WLn709fgtn70yN78sfW2+ttQb0h0R2QctAQXW8713z9CgQr5au0DAKgrLIUTY4HKRxx7XBZXchuD
YAQ6PmXDzQHe3qTWDLqO3tkE7hdWIpuPY/1NFgu3c5eM+SW10WZZEi5PGrjm6gSSrj0RuVFCPYew
MYWveVqc/udOXpJPQ/yrOq2lEiZmueIM15jO1FiIlUAKt0SdE3QrwqXrIbWYENiLxQSIfIY9g5QYb
m8+5caA9ouM/Qj9r+hwDezCNzmzAv+YbX79nuIQZ1RXve8uQNjFrybwCqf0Zfm4aaJQ0PZCOrlbk
HQlSogd P75n TSW9R28MHTLOO7YbKvU/PQAtwBbb1TWdJPp2KOZnQUAqhbm84F9b32qbm2fFXTT
xKJxqyQUfccyuB+81fFOvW8XAjnXDpVCOscAPukmYxHqC9FK/xidstd7LzrZlvvoHpKuE1X2Sf2
3EgbsCTBhcN3nZqk8wwRHQ3tlBTutYJXCb8gWH8vIiPYcMt5bMlLSqkqyPyHK9caUPgn6C9D4zq9
2Fdx/c6mUlv53U3t5fZvie27k5x2DXwkkwp9y+cAS7+UEacZAwUswdbxcJzbPEHXEUkFDWug/Fq
TYl6+rPYLWbwNoJ1MCAwEAAaOBqCBpzAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFKaz
4SsrSbbXc6GqIPUB53NlTKxQMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUprPhKytJttdzoaqU
9QHnc2VMrFAwRAYDVR0gBD0wOzA5BgRVHSAAMDEwLwYIKwYBBQUHAgEWI2h0dHA6Ly9hY2VkaWNv
bSSIZGljb21ncm91cC5jb20vZG9jMA0GCSqGSIb3DQEBBQUAA4ICAQDOLAtSUWImfQwng4/F9tqg
aHtPkI7gpHMvEVNEsk7LncwPel/KzEKbHDZ3LtvoOnzqrs4hTGzz3gvoFNTPbNahXwO9jU8/kzIP
eGYDdwdY6ZXIfj7QeQCM8htRM5u8lOK6e25SLTKeI6RF+7YuE7CLGLHdztUdp0J/Vb77W7tH1Pwk
zQSulgUV1qzOMPPKC8W64iLgpq0i5ALudBF/TP94HTXa5gl06xgSYXcGCRZj6hitoocf8seACQI1
TbCojz2GuHlURwCRiipZ7SkXp7FnFvmuD5uHorLUwHv4FB4D5ISMNUlIFmP8sX+g7tq3PgbUhh8oI
KiMnMCArz+2UW6yyetLHKKGKC3tNSixthT8Icjxn4mcB7trzXtaAWPWkFtPf2Y9fwsZo5NjEFIq
nxQWWOLcptSbFosfQkYuIhypZ+thrkQdIVY9St1686+5DkIaaVbnfj0OLLb6zqvIIDJKZ0IOcMDQj3dcE
I2bw/FWAp/tmGYI12JwOV5vx+qQQEQIHrty1tvuWacNGHk0vFQYXIPKNFHtRQrmjseCNj6nOGOp
MCwXEGCSn1WHEIkQwg9naRHMTh5+Spqtr0CodaxWkHS4oJylcW/c6RrlaQXpuvoDs3zk4E7Czp3o
tkYNbn5XOmeUwssfnHdKZ05phkOTOPu220+DkdRgfks+KzgHVZhepA==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer C: *ES*

Issuer O: *EDICOM*

Issuer OU: *PKI*

Issuer CN: *ACEDICOM Root*

Subject C: *ES*

Subject O: *EDICOM*

Subject OU: *PKI*

Subject CN: *ACEDICOM Root*

Valid from: *Fri Apr 18 18:24:22 CEST 2008*

Valid to: *Thu Apr 13 18:24:22 CEST 2028*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:FF:92:95:E1:68:06:76:B4:2C:C8:58:48:CA:FD:80:54:29:55:63:24:FF:90:65:9B:10:75:7B:C3:6A:DB:62:02:01:F2:18:86:B5:7C:5A:38:B1:E4:58:B9:FB:D3:D8:2D:9F:BD:32:37:BF:2C:15:6D:BE:B5:F4:21:D2:13:91:D9:07:AD:01:05:D6:F3:BD:77:CE:5F:42:81:0A:F9:6A:E3:83:00:AB:2B:2E:55:13:63:81:CA:47:1C:7B:5C:16:57:7A:1B:83:60:04:3A:3E:65:C3:CD:01:DE:DE:A4:D6:0C:BA:8E:DE:D9:04:EE:17:56:22:9B:8F:63:FD:4D:16:0B:B7:7B:77:8C:F9:25:B5:D1:6D:99:12:2E:4F:1A:B8:E6:EA:04:92:AE:3D:11:B9:51:42:3D:87:B0:31:85:AF:79:5A:9C:FE:E7:4E:5E:92:4F:43:FC:AB:3A:AD:A5:12:26:66:B9:E2:0C:D7:98:CE:D4:58:A5:95:40:0A:B7:44:9D:13:74:2B:C2:A5:EB:22:15:98:10:D8:8B:C5:04:9F:1D:8F:60:E5:06:1B:9B:CF:B9:79:A0:3D:A2:23:3F:42:3F:6B:FA:1C:03:7B:30:8D:CE:6C:C0:BF:E6:1B:5F:BF:67:B8:84:19:D5:15:EF:7B:CB:90:36:31:62:C9:BC:02:AB:46:5F:9B:FE:1A:68:94:34:3D:90:8E:AD:F6:E4:1D:09:7F:4A:88:38:3F:BE:67:FD:34:96:F5:1D:BC:30:74:CB:38:EE:D5:6C:AB:D4:FC:F4:00:B7:00:5B:85:32:16:76:33:E9:D8:A3:99:9D:05:00:AA:16:E6:F3:81:7D:6F:7D:AA:86:6D:AD:15:74:D3:C4:A2:71:AA:F4:14:7D:E7:32:B8:1F:BC:D5:F1:4E:BD:6F:17:02:39:D7:0E:95:42:3A:C7:00:3E:E9:26:63:11:EA:0B:D1:4A:FF:18:9D:B2:D7:7B:2F:3A:D9:96:FB:E8:1E:92:AE:13:55:C8:D9:27:F6:DC:48:1B:B0:24:C1:85:E3:77:9D:9A:A4:F3:0C:11:1D:0D:C8:B4:14:EE:B5:82:57:09:BF:20:58:7F:2F:22:23:D8:70:CB:79:6C:C9:4B:F2:A9:2A:C8:FC:87:2B:D7:1A:50:F8:27:E8:2F:43:E3:3A:BD:D8:57:71:FD:CE:A6:52:5B:F9:DD:4D:ED:E5:F6:6F:89:ED:BB:93:9C:76:21:75:F0:92:4C:29:F7:2F:9C:01:2E:FE:50:46:9E:64:0C:14:B3:07:5B:C5:C2:73:6C:F1:07:5C:45:24:14:35:AE:83:F1:6A:4D:89:7A:FA:B3:D8:2D:66:F0:36:87:F5:2B:53:02:03:01:00:01

Basic Constraints *IsCA: true*

Authority Key Identifier *A6:B3:E1:2B:2B:49:B6:D7:73:A1:AA:94:F5:01:E7:73:65:4C:AC:50*

Subject Key Identifier *A6:B3:E1:2B:2B:49:B6:D7:73:A1:AA:94:F5:01:E7:73:65:4C:AC:50*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://acedicom.edicomgroup.com/doc

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *03:95:0F:B4:9A:53:1F:3E:19:91:94:23:98:DF:A9:E0:EA:32:D7:BA:1C:DD:9B:C8:5D:B5:7E:D9:40:0B:43:4A*

X509SubjectName

Subject C: *ES*

Subject O: *EDICOM*

Subject OU: *PKI*

Subject CN: *ACEDICOM Root*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2017-12-01T01:00:00Z

Scheme Service Definition URI

URI *[en]* *http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2001.crt*

URI *[es]* *http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2001.crt*

URI	*[en]*	*http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2002.crt*
URI	*[es]*	*http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2002.crt*

14.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

14.1.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier	*1.3.6.1.4.1.30051.3.1.1*

14.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

14.1.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by the AC ACEDICOM Root*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA ACEDICOM Root*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject O:	*EDICOM*
Subject OU:	*PKI*
Subject CN:	*ACEDICOM Root*

X509SKI

X509 SK I *prPhKytJttdzoaqU9QHnc2VMrFA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

14.1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

14.1.4.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier *1.3.6.1.4.1.30051.3.1.1*

14.1.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

14.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by the AC ACEDICOM Root*

Name *[es]* *Certificados Reconocidos emitidos por la CA ACEDICOM Root*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *EDICOM*

Subject OU: *PKI*

Subject CN: *ACEDICOM Root*

X509SKI

X509 SK I *prPhKytJttdzoaqU9QHnc2VMrFA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2008-11-07T00:00:00Z*

14.1.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

14.1.5.5 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier *1.3.6.1.4.1.30051.3.1.1*

14.2 - Service (granted): Qualified certificates issued by the CAEDICOM01

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by the CAEDICOM01*

Name *[es]* *Certificados Reconocidos emitidos por la CA CAEDICOM01*

Service digital identities

Certificate fields details

Version:

3

Serial Number:

2849013759586421594

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHQDCCBSigAwIBAgIIJ4m662xZS1owDQYJKoZIhvcNAQELBQAwNjEWMBQGA1UEAwwNQ0FFRElD
T00gUm9vdDEPMA0GA1UECgwGRURJQ09NMQswCQYDVQQGEwJFUzAeFw0xNDA3MjIxMTAwNDNaFw0y
NDA1MjIxMDIwMDBaMIGBMRMwEQYDVQQDDApDQUVESUNPTTAxMRIwEAYDVQQFEwlCOTY0OTA4Njcx
DzANBgNVBAoMBkVESUNPTTE4MDYGA1UEBwwvQ2FsbGUgQ2hhcmxlcyBSb2JlcnQgRGFyd2luIDsg
LSA0Njk4MCAtIFBhdGVyYnmExCzAJBgNVBAYTAkVTMIICIjANBgkghkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEAtxnyfUbKXqKaCb/1C5O+xy3RkK8tf6EI8cr5Hk6N53eYGGrIcG/B6L43gbc8/CV
p6pv7VldalAalm56dL9WqHqq6Bvg2DFssYYKcmzRT2gIHYE74/x92m1dn6jo4o8MXi8mvfhyvX4L
7QIlnwqtH1mAMPSB8X8bE9+6azf8zGTKiU8vh836uWY23p3VlwpoFsMFxSTlqU4SnUk7aXrRt9wR
fmVZQFl3/Rc47VHnUPtAgsGZ1zIlBGco035Qh9sk7yQXPm9T1l+xOnsK251vgfinlUpnDomFPaWfy
9t7cmCbnbZXiE3bcKXWf9hy+J0dqHV9mTjf89vmAYRZcvS1F78mnTkRnbuSA8MpE++aU5jc6P
UR8IHbhJaWKJWSsZv2p9S38FP7Clk54dO+FixIOHiQZq5PG7z6oEFZI+YFE3IcwvXrsUlLYwobyj
Ewqyw2rEhTW39YkIQSX2NO2ciHL0M50oJAN/JH/zHusUbtzPmGEhIdccevIcU6N8WxBKR+9rF8Ub
Lv98EOWry+ggXr7VLTnzhQEbJB2xfoWcVqnIDSQ62E8Ydu+VcsB42eLvwQtceR+JKrj2swDGQsO
P6sVt5nsqf98CkacjUaIwroT7CJqCWIjSy4RWk2A1SfmgrTDk8I8bkdI+Ysczzzba5KNtqkoaK
0mFGj3kCAwEAAaOCAgQwggIAMIGTBggrBgEFBQcBAQSBhjCBgzBCBggrBgEFBQcwAoY2aHR0cDov
L2FjZWRpY29tLmVkaWNvbWdyb3VwLmNvbS9jZXJ0cy9jYWVkaWNvbXJvb3QuY2VyMD0GCCsGAQUF
BzABhjFodHRwOi8yb2NzcC5hY2VkaWNvbSlZGljb21ncm91cC5jb20vY2FlZGljb21yb290MB0G
A1UdDgQWBBRtaojtLup1R3A9HZ3k+ZFMo+LBTASBgNVHRMBAf8ECDAGAQH/AgEAMBSGA1UdIwQY
MBaAFBTNKlI4Y6thGei4PaHgWsB15/nLMIGbBgNVHSAEgZMwgZAwgY0GDCsGAQQBgcpjAgMBATB9
ME4GCCsGAQUFBwICMEIeQABDAGUAcgB0AGkAZgBpAGMAYQB0AGkAbwBuACAAUAByAGEAYwB0AGkA
YwBlACAAUwB0AGEAdABlAG0AZQBuAHQwKwYIKwYBBQUHAgEWH2h0dHA6Ly9hY2VkaWNvbS5lZGlj
b21ncm91cC5jb20wQQYDVR0BBDowODA2oDSgMoYwaHR0cDovL2FjZWRpY29tLmVkaWNvbWdyb3Vw
LmNvbS9jYWVkaWNvbXJvb3QuY3IsMAGA1UdDwEB/wQEAwIBhjAjBgNVHREEHDAagRhbY2VkaWNv
bUlBZGljb21ncm91cC5jb20wDQYJKoZIhvcNAQELBQADggIBAD+qPUsRtjlNf0mP14v2GX9bAhGd
DV0acG7AbU5WFIxa3Jo31LWWdXjkJ6/e9dTJnQvzGCIgVrxkpWqFegVBbqJTnPjcCma+YmiLZIT
cWao52q84+EggP4cvPVF4OEWeh2q8Mf0XAQqsTz++DYyLwUmL+SeC3MaRhQvrOvCxdIL6LKomucny
scfVQ5COBwtGgFCm8KIKPGeG1USwsb7sINqFSQ37bWdN2Ney2q8XRtkmyv/quGQjH7yAw552auHgL
c/KyYrEBpqBPtar64B/vyXiCdgqIhRvgnGy9EuD2UdVdo9sxRHDTuTkJ/mXNON4ETw5vFij3DX
ijAmFSd/0zJgcORN8XVJVbxJiTdny38WNpLg8I7AHI1nQ0X3uvIf9zuHjLgN1PuW+UBGDyEAGEKr
XzYuagIFRJgFkhvZ5CArnLEigK6hxhRvgt0GoXwM3qrta56lx6N03PIbnhd1pYTroqJXI6ac8g3
PKerBaleINzLgm/nIfp4Y/1TvEOc2bCrv7DO07lzJKTXcTzFJlnvfeO2Iuy9AC Q8/jigHcdzlkC
PSV7U12mR5APFMZAUaepL+/jDpRt0W3H00Y1JWwhEZa5MCy+1+RJRnNPYklKeFWd8UPuaLANeP
kjo8467kMkI4WxHJgjOz1odXVwZhMnCkPpfdf0hRuFcSMQsk

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer C:

ES

Issuer O:

EDICOM

Issuer CN:

CAEDICOM Root

Subject C:

ES

Subject L:

Calle Charles Robert Darwin 8 - 46980 - Paterna

Subject O:

EDICOM

Subject SERIAL NUMBER:

B96490867

Subject CN:

CAEDICOM01

Valid from:

Tue Jul 22 13:00:43 CEST 2014

Valid to:

Wed May 22 12:20:00 CEST 2024

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:8B:1B:B2:7C:26:CA:89:7A:8A:68:22:2F:D4:2E:4E:FB:1C:B7:FD:19:02:F2:D2:7A:11:FF:E5:F1:CA:F9:1E:4E:8D:E7
:77:98:18:6A:C7:70:6F:C1:E8:BE:37:8E:06:DC:F3:F0:95:A7:AA:72:ED:59:5D:6A:50:1A:22:6E:7A:74:BF:56:A8:7A:AA:E8:1B:E0:D8:31:6C:B1:86:0A:72:6C:D1:4F:68:08:1D:81:3B:E3:FC:7D:DA:6D:5D:9F:A8:E8:E2:8F:
0C:5E:2F:26:BD:F8:72:C1:7E:0B:ED:09:65:9F:0A:AD:1F:59:80:30:F4:81:F1:7F:1B:13:DF:BA:6B:37:FC:CC:64:CA:89:4F:2F:87:CD:FA:B9:66:36:DE:9D:D5:23:0A:68:16:C3:05:C5:24:ED:A9:4E:12:9D:49:3B:69:7A:D1:B7
:DC:11:7E:65:59:40:59:77:FD:17:38:ED:51:E7:50:FB:40:82:A1:99:D7:37:E5:04:67:34:DF:94:21:F6:C9:3B:C9:05:CF:9B:D4:DF:D7:EC:4E:AE:C2:B6:E7:5B:E0:7E:29:E5:52:99:C3:A2:61:4F:69:67:F2:F6:DE:DC:9E:E0:9B:9
D:B6:57:88:4D:DB:78:A5:D6:23:D8:72:F8:9D:1D:A8:75:48:F6:64:E3:16:DF:3D:BE:60:18:45:97:2F:48:71:7B:46:6B:13:91:19:DB:B9:20:3C:32:91:3E:F9:A5:39:8D:CE:8F:51:1F:08:1D:B8:49:69:62:89:59:2B:19:BF:6A:7D:4
B:7F:05:3F:B0:A5:93:9E:1D:3B:E1:62:C6:53:87:89:06:6A:E4:F1:BB:CF:AA:04:15:99:7E:60:51:37:21:CC:2F:5E:BB:14:94:B6:30:A2:1C:A3:13:0A:B2:C3:6A:C4:85:55:B7:F5:89:25:41:25:F6:34:ED:9C:88:72:F4:33:9D:28:2
4:03:7F:24:7F:F3:1E:EB:14:6E:DC:CF:98:61:21:21:D7:1C:7A:F2:1C:53:A3:7C:5B:10:4A:47:EF:6B:17:C5:1B:2E:FF:7C:10:E5:AB:CB:EA:A0:5E:BE:D5:2D:39:F3:85:01:1B:24:1D:B1:7E:85:9C:56:A9:E5:24:34:90:EB:61:3
C:61:DB:BE:55:EB:01:E3:67:8B:CB:04:2D:71:E4:7E:24:AB:63:DA:CC:03:19:0B:0E:3F:AB:15:B7:99:EC:A8:8F:7C:0A:46:9C:8D:46:A5:C2:BA:13:EF:B0:89:A8:25:88:8D:28:F8:45:69:36:03:54:9F:9A:08:93:0E:4F:25:DD:
BF:1D:97:E6:39:CD:CC:F3:FD:B6:B9:28:DB:6A:F2:86:8A:D2:61:46:8F:79:02:03:01:00:01
```


Authority Info Access

http://acedicom.edicomgroup.com/certs/caedicomroot.cer

http://ocsp.acedicom.edicomgroup.com/caedicomroot

Subject Key Identifier

6D:6A:88:F8:2E:EA:7F:2F:CD:C0:F4:76:77:93:E6:45:32:EF:8B:05

Basic Constraints

IsCA: true - Path length: 0

Authority Key Identifier	*14:CD:2A:59:78:63:AB:61:19:E8:B8:3D:A1:E0:5A:C0:75:E7:F9:CB*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.30051.2.3.1.1* *CPS text: [Certification Practice Statement]* *CPS pointer: http://acedicom.edicomgroup.com*
CRL Distribution Points	*http://acedicom.edicomgroup.com/caedicomroot.crl*
Subject Alternative Name	*acedicom@edicomgroup.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*33:9D:15:B1:65:CA:81:61:E4:D3:79:26:18:C6:FD:E8:4E:49:04:D0:46:69:54:1C:EE:6B:D3:33:BC:D5:B5:F4*

X509SubjectName

Subject C:	*ES*
Subject L:	*Calle Charles Robert Darwin 8 - 46980 - Paterna*
Subject O:	*EDICOM*
Subject SERIAL NUMBER:	*B96490867*
Subject CN:	*CAEDICOM01*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-12-01T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

14.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.30051.2.3.2.6*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.30051.2.3.2.4*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.30051.2.3.2.5*

14.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

14.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

14.2.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by the CAEDICOM01*
Name	*[es]*	*Certificados Reconocidos emitidos por la CA CAEDICOM01*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Calle Charles Robert Darwin 8 - 46980 - Paterna*
Subject O:	*EDICOM*
Subject SERIAL NUMBER:	*B96490867*
Subject CN:	*CAEDICOM01*

X509SKI

X509 SK I *bWqI+C7qfy/NwPR2d5PmRTLviwU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

14.2.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.5*

14.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

14.2.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by the CAEDICOM01*

Name *[es]* *Certificados Reconocidos emitidos por la CA CAEDICOM01*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject L: *Calle Charles Robert Darwin 8 - 46980 - Paterna*

Subject O: *EDICOM*

Subject SERIAL NUMBER: *B96490867*

Subject CN: *CAEDICOM01*

X509SKI

X509 SK I *bWqI+C7qfy/NwPR2d5PmRTLviwU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-12-31T23:00:00Z*

14.2.5.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.5*

14.3 - Service (withdrawn): Sellos cualificados de tiempo emitidos por EDICOM

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	[es]	*Sellos cualificados de tiempo emitidos por EDICOM*
Name	[en]	*Qualified timestamps issued by EDICOM*

Service digital identities

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	[en]	*undefined.*
	[es]	*undefined.*

Status Starting Time *2019-12-10T01:00:00Z*

Scheme Service Definition URI

URI	[en]	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	[es]	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

14.3.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name	[es]	*Sellos cualificados de tiempo emitidos por EDICOM*
Name	[en]	*Qualified timestamps issued by EDICOM*

Service digital identities

X509SubjectName

X509SKI

X509 SK I *ziAzKLt9C4McA/Uq1OAj6qYXaGY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-12-01T01:00:00Z*

14.4 - Service (granted): Conservación de sellos electrónicos cualificados proporcionado por EDICOM

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service type description	[en]	*A preservation service for qualified electronic signatures.*

[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name [es] *Conservación de sellos electrónicos cualificados proporcionado por EDICOM*

Name [en] *Preservation of qualified electronic seals provided by EDICOM*

Service digital identities

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2017-12-01T01:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI [es] *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

14.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

14.5 - Service (granted): Servicio cualificado de entrega electrónica certificada EDICOM

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description [en] *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name [es] *Servicio cualificado de entrega electrónica certificada EDICOM*

Name [en] *Qualified electronic registered delivery service EDICOM*

Service digital identities

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2019-02-28T01:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

14.6 - Service (granted): Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q*

Service type description	*[en]*	*undefined.*
	[es]	*undefined.*

Service Name

Name	*[es]*	*Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM*
Name	*[en]*	*Qualified validation service for qualified electronic signatures and qualified electronic seals by EDICOM*

Service digital identities

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2019-02-28T01:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

14.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

14.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

14.7 - Service (granted): Sellos cualificados de tiempo emitidos por TSA EDICOM

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[es]*	*Sellos cualificados de tiempo emitidos por TSA EDICOM*
Name	*[en]*	*Qualified timestamps issued by TSA EDICOM*

Service digital identities

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-12-10T01:00:00Z

15 - TSP: Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)

.

TSP Name

Name	*[en]*	*Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)*
Name	*[es]*	*Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)*

TSP Trade Name

Name	*[en]*	*Ministerio de Defensa de España*
Name	*[es]*	*Ministerio de Defensa de España*
Name	*[en]*	*MDEF*
Name	*[es]*	*MDEF*
Name	*[en]*	*VATES-S2800231I*
Name	*[en]*	*MINISTERIO DE DEFENSA*
Name	*[es]*	*MINISTERIO DE DEFENSA*

PostalAddress

Street Address	*[en]*	*C/ Arturo Soria, 289*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28071*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*C/ Arturo Soria, 289*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28071*

Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.defensa.gob.es*
URI	*[en]*	*mailto:agpmd@oc.mde.es*

TSP Information URI

URI	*[en]*	*http://www.mde.es*
URI	*[es]*	*http://www.mde.es*

15.1 - Service (withdrawn): Qualified Certificates issued by Ministerio de Defensa de España

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by Ministerio de Defensa de España*
Name	*[es]*	*Certificados reconocidos emitidos por CA MINISDEF-EC-WPG*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *111762255326584813916284623438012473554*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHlDCCBXygAwIBAgIQVBSgnoDoTnNMkINpsWvg0jANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQG
EwJFUzENMAsGA1UEChMETURFRjEMMAoGA1UECxMDUEJMRkwFwYDVQQDExBNSU5JU0RFRi1FQy1S
QUlaMB4XDTEwMDkxNTA4MjcyMVoXDTIxMDkxNTA4MjcyMVowRDELMAkGA1UEBhMCRVMxDTALBgNV
BAoTBE1ERUYxDDAKBgNVBAsTA1BLSTEYMBYGA1UEAxMPTUlOSVNERUYtRUMtV1BHMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyVZbU9twB+whhosI7ETOJGtBjE9L88D3HV9mjllvzs2H
iORP4xSJ9KU8Md8j1on/I02GEPHfZzNJ9AcL T+KO07STo FiaGWb6i7yByQs6Dk/9+kYN0VolPE
wgaDIQeFhWU14K00I6sxsIXEXKn4Gi7LodK8kWcKZx271s9/INGsQagS3plxv0VAdJvUPzDEdX4D
iCFGnXHEz4UTryU4K1taKmY5Hb/sxLDvJR4/dKvKsKq1ze8LIlKJbWkHJfZmxRtrUFX1ImIbmpyt
hV/i7JC/ofoSqLJ1+jSflExMcILNZ2n/k1Eudo/6K4PL+dvOV9vPcf3yyPX2vPHzZgFcuwIDAQAB
o4IDfzCCA3swDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFKvjuSGA
W/p2D8dG27CbAtasccqvMB8GA1UdIwQYMBaAFNvVDJ3uHMA/CRl/8N2hB3QAKEQ9MIHzBgNVHSAE
gcswgegwOAYIYIVUAQEBAQEwLDAqBggrBgEFBQcCARYeaHR0cDovL3BraS5tZGVmLmVzL2Nwcy9j
cHMuaHRtMDgGCGCFVAEBAQECMCwwKgYIKwYBBQUHAgEWHmh0dHA6Ly9wa2kubWRlZi5lcy9jcHMv
Y3BzLmb0bTA4BghghVQBAQEBAzAsMCoGCCsGAQUFBwIBFh5odHRwOi8vcGtpLm1kZWYuZXMvY3Bz
L2Nwcy5odG0wOAYIYIVUAQEBAQQwLDAqBggrBgEFBQcCARYeaHR0cDovL3BraS5tZGVmLmVzL2Nw
cy9jcHMuaHRtMDGYBgNVHREEgZAwgY2kgYowgYcxCzAJBgNVBAYTAkVTMQ0wCwYDVQQKEwRNREVG
MQwwCgYDVQQLEwNQS0kxKDAmBgNVBAs TH01pbmlzdGVyaW8gZGUgRGVmZW5zYSBkZSBFc3Bh8WEx
MTAvBgNVBAMTKEVudGlkYWQgZGUgQ2VydGlmaWNhY2lvbiBTdWJvcmRpbmFkYSBXUEcwggGFBgNV
HR8EggF8MIIBeDCCAXSgggFwoIIBbIaBuGxkYXA6Ly8vQ0497TUlOSVNERUYtRUMtUkFJWixDTj1F
Qy1SQUlaLENQPUNEICCDTj1QaWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1D
b25maWd1cmF0aW9uLERDPUVULERDPU1ERSxEQz1FUz9jZXJ0aWZpY2F0ZVJldm9YXRp625MaXN0
P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGfinxkYXA6Ly9sZGFwLmlkZWYu
ZXMvY249TUlOSVNERUYtQ1JMLUVDLVJBSVosT11/9UEtJLE89TURFRixDPUVTP2NlcnRpZmljYXRl
UmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RjbGFzcz1UkxEaXN0cmlidXRpb25Q0n2ludlYvaHR0
cDovL3BraS5tZGVmLmVzL2NvbC9NSU5JU0RFRi1DLkwtRUMtUkFJWi5jcmwwDQYJKoZIhvcNAQEF
BQADggIBAAMqVuSkD0y9XqmvMIG/sShRVmFtuVl/SAH0rdj3n8T15gRZJWOA6Cd0JZFSo2G/bT7P
DBH/58UXMk2xzNrVWLNe9oAH69mfaVmf3MPP5G/CklqOlNv41ey+vN+tVEXAOJBa0b1EnWK3p6jc
6F0VZTPkg/gK+mnVdkmvcf7Yi3RhDhC/AIkb3yQhFuWKoD+FAW8dH0XbxUvlGFiwQ15DHOpsU1W
2Hyd98Btgw9sC1Ip4zNcLvHbFAvLc7v1rvEkPovuIS96Sk/OYRdK6oC2mnFdK9bcZ4VEAS/A0j
7knPmK+F4Y2m9eKa6GBelbEPMhLbGzVT6kF78kml4SFFX2N3Wytr0oBwX4TCuJYLg+D/gvuNR3YP
8P9o+u/KPWV6uRAbdiXhGxMUTJhSI26YH0FKZm4DLytK06L1md86i8sw3xK0JsgwUSLPtT7lP9P9+
jvIAG/zBpO7VMUIY48qApvCYF9uCEla0XtKtih7ts5bKdupqp7Zbb4X+iShDECNFW2PxxIZJnTh
eCUkIRIAsd9SLIZAvQTkZ0zAh+IzMBPYIp1sbiUVxEbw5pOvO73nSRjGEpapkGPJHVDpteRDQ
tNTa23fzD3GOpqWPLUB3hya5yeSbej0w8hnaA/CWOPx5J+qkG53Ek83QuNovsfkpSmkkDdJUCOm
Af6ezPg8
-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN:	*MINISDEF-EC-RAIZ*
Issuer OU:	*PKI*
Issuer O:	*MDEF*
Issuer C:	*ES*
Subject CN:	*MINISDEF-EC-WPG*
Subject OU:	*PKI*
Subject O:	*MDEF*
Subject C:	*ES*
Valid from:	*Wed Sep 15 10:27:21 CEST 2010*
Valid to:	*Wed Sep 15 10:27:21 CEST 2021*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C9:56:5B:53:DB:70:07:EC:21:86:8B:08:EC:44:CE:24:6B:41:8C:4F:4B:F3:C0:F7:1D:5F:66:8C:89:6F:CE:CD:87:88:93:91:3F:8C:79:27:D2:94:F0:C7:7C:8F:5A:27:FC:8D:36:18:43:C7:7D:9C:CD:27:D0:1E:2D:3F:8A:3B:4E:D2:4E:81:5F:B5:A1:96:6F:A7:FB:C8:1C:90:B3:A0:E4:FF:DF:A4:60:DD:15:A2:53:C4:C2:06:83:95:07:85:85:65:35:E0:AD:34:27:AC:6C:95:71:17:2A:7E:06:8B:B2:E8:74:AF:24:59:C2:99:C7:6E:F5:B3:D8:FF:20:D1:AC:41:A8:12:DE:92:31:BF:45:40:74:9B:D4:3F:30:C4:75:7E:03:88:21:46:9D:72:04:CF:85:13:AF:25:38:2B:5D:5A:2A:66:39:1D:BF:EC:C6:D2:C3:BC:94:78:FD:D4:6F:2A:C2:AA:27:37:BC:2C:89:4A:25:B5:A4:7C:88:D9:A7:14:65:AD:41:57:1E:69:61:9A:9C:AD:85:5F:E2:EC:90:BF:A1:FA:12:A8:B2:75:FA:34:9F:94:4C:4C:70:82:CD:67:69:FF:93:51:2E:76:8F:FA:2B:83:CB:F9:DB:CE:57:DB:CF:71:F2:72:C8:F5:F6:BC:F1:F3:66:01:5C:BB:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2*
Authority Key Identifier	*8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D*
Certificate Policies	*Policy OID: 2.16.724.1.1.1.1.1* *CPS pointer: http://pki.mdef.es/cps/cps.htm* *Policy OID: 2.16.724.1.1.1.1.2* *CPS pointer: http://pki.mdef.es/cps/cps.htm* *Policy OID: 2.16.724.1.1.1.1.3* *CPS pointer: http://pki.mdef.es/cps/cps.htm* *Policy OID: 2.16.724.1.1.1.1.4* *CPS pointer: http://pki.mdef.es/cps/cps.htm*
Subject Alternative Name	*CN=Entidad de Certificacion Subordinada WPG, OU=Ministerio de Defensa de Espaa, OU=PKI, O=MDEF, C=ES*
CRL Distribution Points	*ldap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint* *ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint* *http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl*
Key Usage:	*keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *5C:51:24:36:31:18:EE:56:A4:CC:20:BD:31:05:3E:72:9A:B3:01:5E:82:64:8D:FC:77:A8:EA:F4:84:CA:88:3F*

Certificate fields details

Version: *3*

Serial Number: *115761576748069826636472740459696754397*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGvzCCBKcgAwIBAgIQVxbeY5KcuYJKW2ux9N4O3TANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQG
EwJFUzENMAsGA1UEChMETURFRjEMMAoGA1UECxMDUEtlMRIwFwYDVQQDExBNSU5JU0RFRi1FQy1S
QUlaMB4XDTA5MDcxMzE3MTUyOVoXDTEyMDkyMDEwMDAwMFowRDELMAkGA1UEBhMCRVMxDTALBgNV
BAoTBE1ERUYxDDAKBgNVBAsTA1BLSTEYMBYGA1UEAxMPTUlOSVNERUYtRUMtV1BHMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyVZbU9twB+whhos17E/TOJGtBjE9L88D3HV9mjIlvzs2H
iJORPdcS9KU8Md8j1on/I02GEPHfZzNJ9AcL/T+KO07STaFBaGWb67yByQs6Dk/9+kYN0VaIPE
wgaDIQcFhWU14K00I6xsIXEXKn4Gi7LodK8kWcKZx271s9j/NGsQugS3pIxx0VAdJvUPzDEdX4D
iCFGnXIEz4UTryU4K11aKmY5Hb/sxtLDvJR4/dRvKsKqJze8LIlKJbWkftjZpxRlrUFXHmlhmpyt
hVi/7JC/ofoSqLJ1+jSlIExMcILNZ2n/k1Eudo/6K4PL+dvÖV9vPcIJyyPX2vPHzZgFcuwIDAQAB
o4ICgjCCAqYwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFKvjuSGA
Wp2D8dG27Cbv4tasccqvMB8GA1UdIwQYMBaAFIwvVDJ3uIfMA/CRU8Na5ZVDJ3uIfMAOBgNVHSAE
gbEwga4wOAYIYIVUAQEBAQIwLDAqBggrBgEFBQcCARYeaHR0cDovL3BraS5tZGVmLmVzL2Nwcy9j
cHMuaHRtMDgGCGCFVAEBAQEDMCwwKgYIKwYBBQUHAgEWHmh0dHA6Ly9wa2kubWRlZi5lcy9jcHMv
Y3BzLmb0bTA4BghghVQBAQEBBDAsMCoGCCsGAQUFBwIBFh5odHRwOi8vcGtpLm1kZWYuZXMvY3Bz
L2Nwcy5odC0wgzGFBgNVHR8EggF8MIIBeDCCAXSggzFwoIIBbIaBuGxkYXA6L y8vQ0I9TUIOSVNE
RUYtRUMtUkFJWixDTj1FQy1SQUlaLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJI2aWNlcyxD
Tj1TZXJI2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPUVULERDPU1ERSxEQz1FUz9jZXJ0aWZpY2F0
ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9YI1MRGIzdHJpYnV0aW9uU0phbnSGfmxk
YXA6L y8vZGFwLmlkZWYuZXMvY249TUlOSVNERUYtQU1MLUVDL VIBSVos1TU9LEsILE89TURFRixD
PUVTP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RjbGFzcz1jUlxsEaXN0cmli
dXRpb25Qb2ludlYvaHR0cDovL3BraS5tZGVmLmVzL2NybC9NSU5JU0RFRi1DUKwtRUMtUkFJWi5j
cmwwDQYJKoZIhvcNAQEFBQADggIBAA8wLQT2QnckIX3CBmAsGsP580c9m5gD72W7KFLbyzZfiLoT
bc2izhp4lCtmqVp8XNTD9SsPmKIoI/9WjpFcRoB6fcrAW16xM+EmsuAI+Q/1rV/InuyFpleU0fyG0o
wxOwsYrGnB+yY2b1c0uE6W5nivA1G5UBVUtT3dQTH7SIcHTX0vQRgectIvypJhO63dinTNj7zb8j
TFtXTNnY9/gPMRC2/GjJCWK2irYqrUXwiWIxR8XXbeMJ05qBzq8rPi2KVg/uzbemFKKkaE/Mo3or
xoY2wSXr8iA2k9tcrNgWSt04AFxfKzxv6Ioeac9sPfi/87nMcWGg86m1Izu1qBqvDsdYov5x+lcY
YukhnSQIYEesdUHvIhNuRCY6RpTEkN5XQ/ZAWnUP4fyRJ9G013eJpPmB+wsd1FIH600j/BB4VuA
FiQeDK+n09G1SxjjX8OJSqE2DKI+1eOisaBw9uwbmwcYKuwF/HQUQm02ODruXpcylpuHulnOAXhK
FYQzFG6VTFrBJ+k/ZlACoiLCp6FwUGl6QB50KsR+D4UnivVSFRs1FYm/Ea/yG1PzVp6ayrI23Mwui
fx2cZ7RnorD2GYKzLDDxi7tij9Ly4ijeBMgW0nKpV90PV5pXIpDVVUS5aEFaqj+owRMAUm+xcdK1
0+bNdpOrkEFNL+Q1hv1n4MFmWB1q

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *MINISDEF-EC-RAIZ*

Issuer OU: *PKI*

Issuer O: *MDEF*

Issuer C: *ES*

Subject CN: *MINISDEF-EC-WPG*

Subject OU: *PKI*

Subject O: *MDEF*

Subject C: *ES*

Valid from: *Mon Jul 13 19:15:29 CEST 2009*

Valid to: *Thu Sep 20 12:00:00 CEST 2012*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C9:56:5B:53:DB:70:07:EC:21:86:8B:08:EC:44:CE:24:6B:41:8C:4F:4B:F3:C0:F7:1D:5F:66:8C:89:6F:CE:CD:87:88:9
3:91:3F:8C:79:27:D2:94:F0:C7:7C:8F:5A:27:FC:8D:36:18:43:C7:7D:9C:CD:27:D0:1E:2D:3F:8A:3B:4E:D2:4E:81:5F:B5:A1:96:6F:A7:FB:C8:1C:90:B3:A0:E4:FF:DF:A4:60:DD:15:A2:53:C4:C2:06:83:95:07:85:85:65:35:E0
:AD:34:27:AC:6C:95:71:17:2A:7E:06:8B:B2:E8:74:AF:24:59:C2:99:C7:6E:F5:B3:D8:FF:20:D1:AC:41:A8:12:DE:92:31:BF:45:40:74:9B:D4:3F:30:C4:75:7E:03:88:21:46:9D:72:04:CF:85:13:AF:25:38:2B:5D:5A:2A:66:39:1
D:BF:EC:C6:D2:C3:BC:94:78:FD:D4:6F:2A:C2:AA:27:37:BC:2C:89:4A:25:B5:A4:7C:88:D9:A7:14:65:AD:41:57:1E:69:61:9A:9C:AD:85:5F:E2:EC:90:BF:A1:FA:12:A8:B2:75:FA:34:9F:94:4C:4C:70:82:CD:67:69:FF:93:51
:2E:76:8F:FA:2B:83:CB:F9:DB:CE:57:DB:CE:71:F2:72:C8:F5:F6:BC:F1:F3:66:01:5C:BB:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2*

Authority Key Identifier

8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D

Certificate Policies

Policy OID: 2.16.724.1.1.1.1.2

CPS pointer: http://pki.mdef.es/cps/cps.htm

Policy OID: 2.16.724.1.1.1.1.3

CPS pointer: http://pki.mdef.es/cps/cps.htm

Policy OID: 2.16.724.1.1.1.1.4

CPS pointer: http://pki.mdef.es/cps/cps.htm

CRL Distribution Points

ldap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint

ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint

http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

4E:27:9E:AE:24:E4:76:CA:89:50:7D:E8:F5:07:54:EE:57:CB:55:C0:39:4C:AC:7F:9C:A3:4E:C7:6D:47:0E:13

Certificate fields details

Version:

3

Serial Number:

537635824398565544496255232947829069 24

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG7jCCBNagAwIBAgIQK1H9RPudvzRFERgbZObiLDANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQG
EwJFUzENMAsGA1UEChMETURFRjEMMAoGA1UECxMDUEtJMRkwFwYDVQQDExBNSU5JU0RFRi1FQy1S
QUlaMB4XDTA2MDkyMDEwMTc1MloXDTEyMDkyMDEwMTc1MlowRDELMAkGA1UEBhMCRVMxDTALBgNV
BAoTBE1ERUYxDDAKBgNVBAsTA1BLSTEYMBYGA1UEAxMPTUlOSVNERUYtRUMtV1BHMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyVZbU9tuB+whhosI7ETOJGtBjE9L88D3HV9mjIlvzs2H
iJ0RPdc59RUl8Md8j1on/ltl2GEPHZzNJ9AeLT+KO07STsFBaGWb67yByQs6Dk/9+kYN0VadPE
wgaDIQeFhWU14K00J6xsIXEXn4Gi7LodK8kWcKZx271s9j/INGsQagS3pIxx0VAdJvUPzDEdX4D
iCFGnXIEz4UTryU4K11aKmY5Hb/sxtLDvJR4/dRvKsKqJze8LIlKJbWkfIjZpxRlrUFXHmlhmpyt
hVi7JC/ofoSqLJ1+jSHExMcILNZ2n/k1Eudo/6K4PL+dvOV9vPcIyyPX2vPHzZgFcuwIDAQAB
o4IC27CCAtUwDwYDVR0TAQH/BAUwAwEB2zAOBgNVHQ8BAR8EBAMCAQYwHQYDVR0OBBYEFKvjuSGA
Wp2D8dG27CbrAtascqyMHwGA1UdIwR1MHOAFIwvYDI5uHMA3CRU8N2bB3QAKEQ9oLmkRzBFMQsw
CQYDVQQGEwJFUzENMAsGA1UEChMETURFRjEMMAoGA1UECxMDUEtJMRkwFwYDVQQDExBNSU5JU0RF
Ri1FQy1SQUlaghAAnHipt3bG65GzzOlied5MIG8BgNVHSABAf8EgbEwga4wOAYIYIVUAQEBAQIw
LDAqBggrBgEFBQcCARYeaHR0cDovL3BraS5tZGVmLmVzL2Nwcy9jcHMuaHRtMDgGCGCFVAEBAQED
MCwwKgYIKwYBBQUHAgEWHmhldHA6Ly9wa2kubWRlZ25lcy9jcHMvY3BzLmht0TA4BghghVQBAQEB
BDAsMCoGCCsGAQUFBwIBFh5odHRwOi8vcGtpLm1kZWYuZXMvY3BzL2Nwcy5odG0wggFUBgNVHR8E
ggFLMIIBRzCCAUOgggE/oIIBO4aBuGxkYXA6Ly8vQ049TUlOSVNERUYtRUMtUkFJWixDTj1FQy1S
QUlaLENOPUNEUCSDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj11Db25m
aWd1cmF0aWNuLERDPUVULERDPUJERSxEQe1FUe9ZX0taWZpY2F0ZVJdm9jYXRpb25MaXN0P2Jh
c2U/b2lqZWN0Y2xhc3M9YJMRGlzdHJpYnV0aW9uUG9pbnSGfmxkYXA6Ly9sZGFwLm1kZWYuZXMv
Y249TUlOSVNERUYtQ1JMLUVDLVJBSVosT1U9UEtJLE89TURFRixDPUVTP2NlcnRpZmljYXRlUmV2
b2NhdGlvbkxpc3QYYmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Ob2ludDANBgkqhkiG
9w0BAQUFAAOCAgEAH+SRAZUjRY+pcmxvnfygk/92Yf4cNW8BddbQvCDs8GXAjmECxmFzqvLcmLD
VQSOgoeEDI8RaT3cz6V7finEN59dFmq4JYcxgNGgsOLVKgcC402qKA2g1KYQO3glQB8Pk31dIjaWZ
AsK6mkV7hbZ1yW2lq0C3GtbFRDXBdYoRDi81cnYJZxB0MlPxUeVWlyr2bKuFv8rK5S5g3ZD0XHlD
sHxvfcq1Q5jFSzUVzvXXtk9gF6Xrn/cgEcqGQEx/6eOMewGFRy5lE3yggYDQrcdadfxR3yZQxP/f
OxwpEPZmlUwYiSzIH2VozAVZQ8Xtbz7RZAKAHi7UKI1Sy6JHkUTeERxVksL6M/GjzDPNH12e8efp
Pt/5jOjv+qmohDAzsAk17lDJTVoQwrTB69NMTfa9+IBN+kqEJvQGDJJCJFU4pCVrPpi8FPX7yf4
emTF3yVCZzfvLHLDFkMPEl9ZNlG8bdbldXSLqwU1RIFgyr4DAFbAUaBZtg/ETi2xKcgbjoT7Y2Jo
tsBNa98Jn1QaZ5KZwuiDa60lyJNgyxhgy3DGuxYZdBW8ohyQ+ZzvZL+YK9KeimCDjLWf03IT1kQS
GPF3MAvLJpDX02Aq0VYaVYzb/csIMiNXEx/YnvU93UM+VWOvtPNyU6OEmgrPb8LiPUMcb0HgpzBC
4nAtFtWMIdfI0Yo=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA1withRSA

Issuer CN:

MINISDEF-EC-RAIZ

Issuer OU:

PKI

Issuer O:

MDEF

Issuer C:

ES

Subject CN:	*MINISDEF-EC-WPG*
Subject OU:	*PKI*
Subject O:	*MDEF*
Subject C:	*ES*
Valid from:	*Wed Sep 20 12:17:52 CEST 2006*
Valid to:	*Thu Sep 20 12:17:52 CEST 2012*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C9:56:5B:53:DB:70:07:EC:21:86:8B:08:EC:44:CE:24:6B:41:8C:4F:4B:F3:C0:F7:1D:5F:66:8C:89:6F:CE:CD:87:88:93:91:3F:8C:79:27:D2:94:F0:C7:7C:8F:5A:27:FC:8D:36:18:43:C7:7D:9C:CD:27:D0:1E:2D:3F:8A:3B:4E:D2:4E:81:5F:B5:A1:96:6F:A7:FB:C8:1C:90:B3:A0:E4:FF:DF:A4:60:DD:15:A2:53:C4:C2:06:83:95:07:85:85:65:35:E0:AD:34:27:AC:6C:95:71:17:2A:7E:06:8B:B2:E8:74:AF:24:59:C2:99:C7:6E:F5:B3:D8:FF:20:D1:AC:41:A8:12:DE:92:31:BF:45:40:74:9B:D4:3F:30:C4:75:7E:03:88:21:46:9D:72:04:CF:85:13:AF:25:38:2B:5D:5A:2A:66:39:1D:BF:EC:C6:D2:C3:BC:94:78:FD:D4:6F:2A:C2:AA:27:37:BC:2C:89:4A:25:B5:A4:7C:88:D9:A7:14:65:AD:41:57:1E:69:61:9A:9C:AD:85:5F:E2:EC:90:BF:A1:FA:12:A8:B2:75:FA:34:9F:94:4C:4C:70:82:CD:67:69:FF:93:51:2E:76:8F:FA:2B:83:CB:F9:DB:CE:57:DB:CF:71:F2:72:C8:F5:F6:BC:F1:F3:66:01:5C:BB:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2*
Authority Key Identifier	*8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D*
Certificate Policies	*Policy OID: 2.16.724.1.1.1.1.2* *CPS pointer: http://pki.mdef.es/cps/cps.htm* *Policy OID: 2.16.724.1.1.1.1.3* *CPS pointer: http://pki.mdef.es/cps/cps.htm* *Policy OID: 2.16.724.1.1.1.1.4* *CPS pointer: http://pki.mdef.es/cps/cps.htm*
CRL Distribution Points	*ldap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint* *ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*49:D2:25:4C:1C:9F:02:F1:E6:B5:CC:DE:9C:2E:B7:79:CD:0D:A3:D9:93:90:8F:6D:8D:43:7B:57:C9:A2:D4:A7*

X509SubjectName

Subject CN:	*MINISDEF-EC-WPG*
Subject OU:	*PKI*
Subject O:	*MDEF*
Subject C:	*ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-07-01T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

15.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.1.1.1.2.14*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.1.1.1.3.14*

15.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by Ministerio de Defensa de España*

Name *[es]* *Certificados reconocidos emitidos por CA MINISDEF-EC-WPG*

Service digital identities

X509SubjectName

Subject CN:	*MINISDEF-EC-WPG*
Subject OU:	*PKI*
Subject O:	*MDEF*
Subject C:	*ES*

X509SKI

X509 SK I	*q+O5IYBb+nYPx0bbsJuIC1qxyrI=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

15.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.1.1.1.2.14*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.1.1.1.3.14*

15.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by Ministerio de Defensa de España*
Name	*[es]*	*Certificados reconocidos emitidos por CA MINISDEF-EC-WPG*

Service digital identities

X509SubjectName

Subject CN:	*MINISDEF-EC-WPG*
Subject OU:	*PKI*
Subject O:	*MDEF*
Subject C:	*ES*

X509SKI

X509 SK I	*q+O5IYBb+nYPx0bbsJuIC1qxyrI=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2009-04-30T00:00:00Z*

15.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.1.1.1.2.14*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.1.1.1.3.14*

15.2 - Service (granted): Qualified Certificates issued by Ministerio de Defensa de España 2016

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by Ministerio de Defensa de España 2016*

Name *[es]* *Certificados cualificados emitidos por CA DEFENSA-EC-WPG2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *104027222427762634661741286331660447518*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIlOzCCBiOgAwIBAgIQTkLqDaHCwT9X0Rh/+u0vHjANBgkqhkiG9w0BAQsFADBvMQswCQYDVQQG
EwJFUzEeMBwGA1UECgwVTUlOSVNURVJlTyBERSBERUZFTlNBMQwwCgYDVQQLDANQS0kxGDAWBgNV
BGEMD1ZBVEVTLVMyODAwMjMxSTEYMBYGA1UEAwwPREVGRUSTQS1FQy1SQUlaMB4XDTE2MDkwODA3
NTEyN1oXDTI3MDkwODA3NTEyN1owcjELMAkGA1UEBhMCRVMxHjAcBgNVBAoMFUJlTkTlTVEVSSU8g
RtUgREVGRUSTQTEMMAoGA1UECwwDUEtlMRgwFgYDVQQhDA9WQVRtUy1TMjgwMDIzMUkxGzAZBgNV
BAMMEkRFRkVOU0EtRUMtV1BHMjAxNjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJqP
2ugn6fb/u2Kt1aqdZsUh7zYuuTuuBAtJHTZAaYiMT3dimIQ/cmSX/cjNrxFJWANe6Kk8Khrt+lUl
Jp/Srp1V1gINsxZcNxtMArnwhfjTANZU3kivyc/dRzCPtZHzSF/BVtT27Cv4c0Fy5vtOnser1Qi
yznCEwLfVDWOlfp1Apq1Im1/PtQgQ4YJW/8kggqeqCmCUBeT7XpnobPNNcAZbtEkdmYRtzZdH0P+
10SkGKu1WpVC3fizJoAgRMlhpy3G3n4cNB3DdSc/39wxyP3TqVsObkIp/w/SyjhlFIYs/jovlgrz
CWw/Do/FilA VI0YphxU5rFyZ4E01GKJCTNO48oSzvRKU340lOFgFwopDBQhLhZjGgk1dGVMsfxAq
pMDGhZOz1+096SGV+aaM2B4ih+drGFUPvrwydKZvF/grBNT60yTZHAwrpOCT62/zJ6oGSnHCR/rx
DJHFGmnPLnuA2f+KAb9bNlydPraQ0Fiq6G1UTFwq6G7MSguf5VmK6jAOMOhxLjKimUEWBnZqKtAt
i8Ut7mfF9NCzmBHWAjUPKSq2cFyVCX8mHVVlk+yTyDmv8Ch853ao6+kH2PoWcpzg2wj21KcBN7G+
bgSlXZnetaqPdjPkYMItoQmERmGb51Prahq8FEziLf80Gs0mFtodZq0ZOfF7HVXw782evQVBAgMB
AAGjggLOMIICyjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQU
kVSYiMS+YZY0juV3vxd0D+7qCNIwHwYDVR0jBBgwFoAUjCOUMnc4cwD8JFTw3aEHdAAoRD0wggegG
A1UdIASB4DCB3TCB2gYEVR0gADCB0TAiBggrBgEFBQcCARYWaHR0cDovL3BraS5ZGUuZXMvZHBj
LzCBqgYIKwYBBQUHAgIwgZ0agZpDZXJ0aWZpY2FkbyBkZSBsYSBFbnRpZGFkIGRlIENlcnRpZmlj
YWNpb24gU3Vib3JkaWS5hZGEgVlBHMjAxNiBkZWwgTWluaXN0ZXJpbyBkZSBEZWZlbnNhIGRlIEVz
cGHxYSAoUEUREVGLCBDSUYgU/zI4MDAyMzFJLCBBenR1cm8gU29yaWEgMjg5ID4MDcxIE1hZHIp
ZCkuMIG0BgNVHREEgawwgamBFWJhaWw6IGFnaGlkQG9hLmlkZSSlceSSBzCBjDELMAkGA1UEBhMC
RVMxDTALBgNVBAoMBE1ERUYxDDAKBgNVBAsMA1BLSTEpMCcGA1UECwwgTWluaXN0ZXJpbyBkZSBE
ZWZlbnNhIGRlIEVzcGHDsWExNTAzBgNVBAMMLEVudGlkYWQgZGUgQ2VydGlmaWNhY2lvbiBTdWJv
cmRpbmFkYSBXU/EcyMDE2MlHBBgNVHR8Egbkwgb1YwgbOggbCgga2GLWh0dHA6L y9wa2kubWRlLmVz
L2NybC9ERUZFTlNBLUNSTC1FQy1SQUlaLmNybIZ8bGRhcDovL2ck YXAubWRlLmVz L2NuPURFRkVO
U0EtQ1JMLUVDLVJBSVosT1U9UEtlLE89TURFRxDPUVTP2NlcnRpZmlj YXRlUmV2b2NhdGlvbkxp
c3Q/YmFzZT9vYmplY3RjbGFzcz1jUlkxEaXN0cmlidXRpb25Qb2ludDANBgkqhkiG9w0BAQsFAAOC
AgEADCNSOd6TNLUz8U4J8JpD0k83XtOme8tE3xmykIp1TnMV7geeNs4Klo+jsUYOqktE1iPxtDD
c38OoqUm50lm7YR72fjIL NsdAAmrKP6UCAYPG2wZ2ZONJKrUs13wQ+CpM5bzUc1EscFUoMyIp4Q
k9MFH1MufnKg8UmCX/JWj4k8bhGHZFYX8fOmz6N6xjuyIKXgto83wLtbe9r+jHmeRNORz4swIf
uZl8T/rVXWgqIoJebXpK2M1sD6ZHlQKBQv77OlnqhZwrGhOnWkbVi5ALW/ZUPdbmIU1rW12BDGvD
E6Kqo3k4VSqbNQSMkryffmt8PoGgXOKzlc/eiycVsdbV5UOBdWAeXDZLtQNBYLsu7Jb6xxBSBMA
Tv6SMHGxL5CLVjgTA9Sze8psGGrTMqVE21bsQCD2I1wQhw44gP6WBSHyfjy01+tfIV+SXHAGsAw
ol63O4ygEDhqjKMwnJd0N8M5/uQd0YyO+0e01FtWBut37bVJRMNw4B9MRayiJ47zUxn+dJR46CsE
00ntaKTGU5VlgQYtHbc8wdWStGmyL7nhatYZ/KJQONFgDbXX5a/gEIINNOeSTdmvxnjl3mZ45WIF
jA6QtrFclhhRYafMuxf/q+Qw4U9wxyjw8L72EBTU7fa7kLiYDgs73fmpZcR2yRy9bfi0p7XRoVS
CTo=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DEFENSA-EC-RAIZ*

Issuer 2.5.4.97: *VATES-S2800231I*

Issuer OU: *PKI*

Issuer O: *MINISTERIO DE DEFENSA*

Issuer C: *ES*

Subject CN: *DEFENSA-EC-WPG2016*

Subject 2.5.4.97: *VATES-S2800231I*

Subject OU: *PKI*

Subject O: *MINISTERIO DE DEFENSA*

Subject C: *ES*

Valid from: *Thu Sep 08 09:51:27 CEST 2016*

Valid to: *Wed Sep 08 09:51:27 CEST 2027*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9A:8F:DA:E8:27:E9:F6:FF:BB:62:AD:D5:AA:9D:66:C5:21:EF:36:2E:B9:3B:AE:04:0B:49:1D:36:40:69:88:8C:4F:77:62:98:84:3F:72:64:97:FD:E2:4D:AF:11:49:58:03:5E:E8:A9:3C:2A:1A:ED:F8:85:25:26:9F:D2:AE:9D:55:D6:09:4D:B3:16:71:37:1B:4C:02:B9:F0:85:F8:D3:00:D6:74:DE:48:AF:C9:CF:DD:47:30:8F:7D:91:F3:48:5F:C1:55:F4:F6:EC:2B:F8:73:41:72:E6:FB:4E:9E:C7:AB:D5:0F:E2:CB:39:C2:13:02:DF:54:35:8E:95:FA:58:02:9A:93:9B:5F:CF:89:08:10:E1:82:56:27:CB:6A:82:A7:AA:0A:DB:42:50:17:93:ED:7A:6F:A2:13:CD:35:C0:19:6D:F1:24:76:66:11:B7:36:5D:1F:43:FE:D7:44:A4:18:AB:B5:5A:95:42:DD:F8:B3:26:80:20:44:C2:21:A7:2D:C6:DE:7E:1C:34:1D:C3:77:97:BF:DF:DC:31:C8:FD:D3:A9:5B:0E:6E:42:29:FF:0F:D2:CA:38:48:16:56:2C:1E:3A:2F:96:0A:F3:09:6C:3F:0E:8F:C5:8A:50:15:23:46:29:87:15:39:AC:5C:99:E0:4D:35:18:A2:42:4C:D3:B8:F2:84:B3:BD:12:94:DF:8D:08:38:58:05:C2:8A:43:05:08:4B:85:98:C6:82:4D:5D:19:53:2C:7F:10:2A:A4:C0:C6:85:93:B3:D7:ED:3D:E9:21:95:F9:A6:8C:D8:1E:22:87:E7:6B:18:55:0F:BE:BC:32:74:A6:6F:17:F8:2B:04:D4:FA:D3:24:D9:1C:0C:22:A4:E0:93:EB:6F:F3:27:4A:06:4A:71:C2:47:FA:F1:0C:91:C5:1A:69:CF:2F:3B:80:D9:FF:91:02:1F:61:36:5C:9F:3E:B6:90:D0:5B:6A:E8:6D:48:4C:5C:20:E8:6E:CC:4A:0B:9F:B1:59:8A:EA:30:0E:30:E6:F1:2E:32:A2:99:41:16:06:76:6E:F2:D0:2D:8B:C5:2D:EE:67:C5:F4:D0:B3:98:11:D6:02:35:0F:29:2A:B6:70:5C:95:09:7F:26:1D:55:62:93:EC:93:C8:39:AF:F0:28:7C:E7:76:A8:EB:E9:07:D8:FA:16:72:9C:E0:DB:08:F6:D4:A7:01:37:B1:BE:6E:04:A5:5D:99:DE:B5:AA:8F:76:33:E4:60:C9:6D:A1:09:84:46:61:9B:E7:53:EB:6A:1A:BC:14:4C:E2:2D:FF:34:1A:CD:26:16:DA:1D:66:AD:19:39:F1:7B:1D:55:F0:EF:CD:9E:BD:05:41:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

91:54:98:88:CF:3E:55:96:34:8E:E5:77:BF:17:74:0F:EE:EA:08:D2

Authority Key Identifier

8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://pki.mde.es/dpc/

CPS text: [Certificado de la Entidad de Certificacion Subordinada WPG2016 del Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).]

Subject Alternative Name

mail: agpmd@oc.mde.es

CN=Entidad de Certificacion Subordinada WPG2016, OU=Ministerio de Defensa de España, OU=PKI, O=MDEF, C=ES

CRL Distribution Points

http://pki.mde.es/crl/DEFENSA-CRL-EC-RAIZ.crl

ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

81:44:06:33:1B:97:9F:B1:4E:87:D1:CB:38:ED:0E:F2:BB:5B:EE:0A:1E:72:89:37:D6:BD:D5:D4:94:FC:D5:E6

X509SubjectName

Subject CN:

DEFENSA-EC-WPG2016

Subject 2.5.4.97:

VATES-S2800231I

Subject OU:

PKI

Subject O:

MINISTERIO DE DEFENSA

Subject C:

ES

X509SKI

X509 SK I

kVSYiM8+VZY0juV3vxd0D+7qCNI=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-10-08T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

15.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

15.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

15.2.4 - History instance n.1 - Status: withdrawn

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by Ministerio de Defensa de España 2016*
Name	*[es]*	*Certificados cualificados emitidos por CA DEFENSA-EC-WPG2016*

Service digital identities

X509SubjectName

Subject CN:	*DEFENSA-EC-WPG2016*
Subject 2.5.4.97:	*VATES-S2800231I*
Subject OU:	*PKI*
Subject O:	*MINISTERIO DE DEFENSA*

Subject C: *ES*

X509SKI

X509 SK I *kVSYiM8+VZY0juV3vxd0D+7qCNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Status Starting Time *2017-07-01T22:00:00Z*

15.2.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.2.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by Ministerio de Defensa de España 2016*

Name *[es]* *Certificados cualificados emitidos por CA DEFENSA-EC-WPG2016*

Service digital identities

X509SubjectName

Subject CN: *DEFENSA-EC-WPG2016*

Subject 2.5.4.97: *VATES-S2800231I*

Subject OU: *PKI*

Subject O: *MINISTERIO DE DEFENSA*

Subject C: *ES*

X509SKI

X509 SK I *kVSYiM8+VZY0juV3vxd0D+7qCNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-05-10T00:00:00Z*

15.2.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16 - TSP: Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.

.

TSP Name

Name	*[en]*	*Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.*
Name	*[es]*	*Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.*

TSP Trade Name

Name	*[en]*	*Izenpe, S.A*
Name	*[es]*	*Izenpe, S.A*
Name	*[en]*	*IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Name	*[es]*	*IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Name	*[en]*	*VATES-A01337260*
Name	*[en]*	*IZENPE S.A.*

PostalAddress

Street Address	*[en]*	*Avenida del Mediterráneo, 14*
Locality	*[en]*	*Vitoria-Gasteiz*
State Or Province	*[en]*	*Álava*
Postal Code	*[en]*	*1010*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Avenida del Mediterráneo, 14*
Locality	*[es]*	*Vitoria-Gasteiz*
State Or Province	*[es]*	*Álava*
Postal Code	*[es]*	*1010*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.izenpe.com*

URI	*[en]*	*mailto:izenpe@izenpe.eus*
URI	*[en]*	*http://www.izenpe.eus*

TSP Information URI

URI	*[en]*	*http://www.izenpe.eus/s15-home/en/*
URI	*[es]*	*http://www.izenpe.eus/s15-home/es/*

16.1 - Service (granted): Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)*
Name	*[es]*	*Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *113337510715436163020379579576825479821*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHRTCCBS2gAwIBAgIQVUQCtMaN0r1Jo6pasF0CjTANBgkqhkiG9w0BAQUFADA4MQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMuQS4xEzARBgNVBAMMCklôZW5wZS5jb20wHhcNMDkwMjI0
MDgwNTQ2WhcNMzcxMjEyMjMwMDAwWjCBpzELMAkGA1UEBhMCRVMxFDASBgNVBAoMC0laRU5QRSBT
LkEuMTowOAYDVQQLDDFOWlogWml1cnRbZ2lyaSBwdWJsaWtvYSAtIENlcnRpZmljYWRvIHB1Ymxp
Y28gL0NJMUYwRAYDVQQDDD1LZXJyaXRhciBldGEgRXJha3VuZGVlbiBDQSAtIENBIGRlIENpdWRh
ZGFub3MgeSBFbnRpZGFkZXMgKDQpMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA36d+
iYHzm+LCg6MulPryEGJZQlYmFGgbMd3rLP/o7Rkr1settF1JxctyVQD9Och3a0rwPZZfgtpw1DEV
qn5k2VdXlSEMTqWoNj/dZCDojbl8aN4K2clSjcAZSp7okuAeoM9N6Z1u3O7cgJh+BhDjdlUz801B
Fi4G4mfryuQhPGyP/HrSU+wXAJgsOD5OqMFU1VM6+M7Ws7s4mdWx2eNb2uuIKK5tjUNt6v92dac
0KD8IZJmIwFcF0Bbw396Lnyy45PCqrs5ME0l4i7aYYOvsmyq1DFWlOQGVkIhGd99+fybDM0s+k5Q1
tAzUeLCegS5PyL3ErVc2gIX9b0UqXvFI0lfKs4+Cy0Z3qzBdyewwK5+edxdSUFws//lc14VfWzNi
X1tc86OEUuFEBBTNeMZjvbAIxRXynrcDnPSlMck0JWYkÚNHqKicoS1TTO+oB9md0u6gD7DNpQkay
zSfTwi3gHsTTYRWOX+Pj2WWigW7+sYiSOTbTRxmrxXe8WxRsSK9uz+ziq4RcwF4841WQ5LSZwozx
v51ykcXYHn/fcdPZmrLbD3UiMrLXsKi8N5VA+veY6JUIc1/N35AxmDytDeIUe5vjaGOqC6MLv
gLoGIlRqKO2v2+C+x49oLewbVnIkrQhlFiZmS+CW9dzJCgLE0BPYa4FTisbIrp5cMlcOjzkCAwEA
AaOCAdkwggHVMIHHBgNVHREEgb8wgbyGFWh0dHA6Ly93d3cuaXplbnBlLmNvbYEPaWSmb0BpemVu
cGUuY29tpIGRMIGOMUcwRQYDVQQKDD5JWkVOUEUgUy5BL1AtIENJRjBBMDEzMzcyNjAtUk1lcmMu
Vml0b3JlbYS1HYXN0ZW16IFQxMDU1IEY2MiBTODFDMEEGA1UECQwK0JXZkYSBkZWwgTWVkaXRlcnlh
bmVvIEV0b3JlaWRlYSAxNCAtIDAxMDEwIFZpdG9yaWEtR2F2adGVpejAPBgNVHRMBAf8EBTADAQH/
MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUpBcdTmXX74eVLn+OuhXLBYvTjH0wHwYDVR0jBBgw
FoAUHRxIDgjyJXu0kc/ksbHmvVV0bAUwOgYDVR0gBDMwMTAvBgRVHSAAMCcwzJQYIKwYBBQUHAgEW
GWh0dHA6Ly93d3cuaXplbnBlLmNvbS9jcIMwNwYIKwYBBQUHAQEEKzApMCcGCCsGAQUFBzABhhto
dHRwOi8vb2NzCS5pemVucGUuY29tOgwOTQwMwYDVR0fBCwwKjAooCagJIYiaHR0cDovL2NvbCSp
emVucGUuY29tL2NnaS1ia W4vYXJsMjANBgkqhkiG9w0BAQUFAAOCAgEAZC16vtzzZkWSRNXwSE4W
Hp4j+zMNRFBTobG2aYO5MD8XRneycEqWkqAhOPwr4QUL+qX2m9nmQgxzrRMZM1Myi/IIcpyImlCp
FnktFi5zlPkksJOyVcA7dG96MLizhsIAud/exqNTnI1OBBvZwPqVhSjT4L6aVPOF53S3gaiB5V/
c+r/prqj/nLaBdUlb6u7i0zf6n5/VQsDy3BEJb/uBHxRgJsgsTTob4AGTkh3kFx9MYnuw3TS7Ywt
yubCSpO3sXD8Smpu9WKD3GkWbx0fM0bfaNWPQJ+tsDo2587IO33SJjrCBIwTMekBiG7kp5Pg9cUI
pj0QkXIeIN6229xyBeSXsrkxzhdci68AhmiZ0y5uc2bXNxrcbzt6VDwzlu3IZL9UOAAXlbFddvzI
UuXphbYKKXRXLPgP4l8Dp4xF/N6GIvF/w31a66nKOyagsyrIJkRvUk09Ev1vbYWs44jTcbdOoH38
E3JIHSQF68z9SZ1IV0SekMzuhi8xLN3VNo3IDRSB0jwsan1RrLPvX2IhIM7IL/eaeL5/Rds3Qotz
InaPC/XlIRTrSr0GkC4N5RQQhaSJvoBh7ru9So4ZDbQlVejM0v13i+bn0iLrd9rt7lU6LUx+8IX
1iy+1Ipi+wijZhX5oN+6/06l8kxw+c1216JtImZBHGUKwjH8d5E3KYQ=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Izenpe.com*

Issuer O: *IZENPE S.A.*

Issuer C: *ES*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Valid from: *Tue Feb 24 09:05:46 CET 2009*

Valid to: *Sun Dec 13 00:00:00 CET 2037*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DF:A7:7E:89:81:F3:9B:E2:C2:83:A3:2E:94:FC:B2:10:62:59:42:56:26:14:68:1B:31:DD:EB:2C:FF:E8:ED:19:2B:D6:C7:AD:B4:5D:49:C5:CB:72:55:00:FD:39:C8:77:6B:4A:F0:3D:96:5F:82:DA:70:D4:31:15:AA:7E:64:D9:57:57:23:91:0C:4E:A5:A8:36:3F:DD:64:20:E8:8D:B2:3C:68:DE:0A:D9:C9:52:8D:E0:19:4A:9E:E8:92:E0:1E:A0:CF:4D:E9:9D:6E:DC:EE:DC:80:98:7E:06:10:E3:74:85:33:F3:4D:41:16:DE:06:E2:67:EB:CA:E4:21:3C:6C:8F:FC:7A:D2:53:EC:17:00:98:2C:38:3E:4E:A8:C1:65:27:55:4C:EB:E3:3B:5A:CE:F3:E2:67:56:C7:67:8D:6F:6B:AE:94:A2:B9:B6:35:0D:B7:AB:FD:D9:D6:9E:D0:A0:FC:25:92:66:0F:01:5E:17:40:5B:C3:7F:7A:D6:7C:B2:E3:93:C2:72:9B:39:30:4D:38:8B:B6:95:60:EB:EC:9B:2A:B5:0C:55:88:39:01:95:90:88:46:77:DF:7E:7F:28:43:33:4B:3E:93:94:35:B4:0C:D4:78:B0:9E:81:2E:4F:C8:BD:C4:AD:57:36:82:55:FD:6F:45:2A:5E:F1:48:D2:57:CA:B3:8F:82:CB:46:77:AB:30:5D:C9:EC:30:2B:9F:9E:77:17:52:50:5C:2C:FF:F9:5C:D7:85:5F:5B:33:62:5F:5B:5C:F3:A3:84:52:E1:44:04:14:CD:78:C6:63:BD:B0:08:C5:15:F2:9E:B7:83:9C:F4:A5:31:E9:34:25:66:24:50:D1:EA:2A:27:28:4B:54:D3:3B:EA:01:F6:67:74:BB:A8:03:EC:33:69:42:46:B2:CD:27:D3:C2:2D:E0:1E:C4:D3:61:15:8E:5F:E3:E3:FF:65:96:8A:05:BB:FA:C6:22:48:E4:DB:4D:1C:66:AF:15:DE:F1:6C:51:B1:22:BD:BB:3F:B3:8A:AE:11:73:01:78:F3:85:90:E4:B4:99:C2:8C:F1:BF:9D:72:29:C5:FF:60:79:FF:7F:17:7F:3D:99:AF:2D:B0:F7:51:F3:2B:91:7B:0A:8B:C3:79:54:0F:AF:79:8E:89:51:F7:B5:FC:DD:F9:03:19:83:CA:B0:DE:95:47:B9:BE:3B:06:3A:A0:BA:33:F2:EF:80:BA:06:20:84:6A:28:ED:AF:DB:E0:BE:C7:8F:68:2D:EC:1B:56:72:64:AD:08:48:16:D6:66:4B:E0:96:F5:DC:C9:0A:02:C4:D0:13:D8:6B:81:53:8A:C6:C8:CE:9E:5C:32:57:0E:8F:39:02:03:01:00:01

Subject Alternative Name

http://www.izenpe.com

info@izenpe.com

STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints *IsCA: true*

Subject Key Identifier *A4:17:1D:4E:65:D7:EF:87:95:2E:7F:8E:B8:75:CB:05:8B:D3:8C:7D*

Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.izenpe.com/cps

Authority Info Access *http://ocsp.izenpe.com:8094*

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *26:26:B1:95:63:BC:78:D9:B1:44:2B:93:CE:98:D1:4A:1E:4B:74:26:4A:CC:90:22:2F:1F:3C:23:85:C2:73:37*

Certificate fields details

Version: *3*

Serial Number: *44226866073358392262219520495746478787*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHQTCCBSugAwIBAgIQIUXL2bEFUA5MvqVCVTrywzALBgkqhkiG9w0BAQswODELMAkGA1UEBhMC
RVMxFDASBgNVBAoMC0laRU5QRSBTLkEuMRMwEQYDVQQDDAplemVucGUuY29tMB4XDTEwMTAyMDA4
MTYwMloXDTM3MTIxMjIzMDAwMFowgacC2AIBgNVBAYTAkVTMRQwEgEYDVQQKDAtJWkVOUEUgUy5B
LjE6MDgGA1UECwwxTlpaIFppdXJ0YWdpcmkgcHVibGlrb2EgLSBDZXJ0aWZpY2FkbyBwdWJsaWNv
IFNDSTFGMEQGA1UEAwwvSGVycmI0YXlgZXRhIEVyYWi1bmRlZW4gQ0EgLSBDQSBkZSBDaXVkYWRh
bm9zIHkgRWS9uWRhZGVzIC gtKTCCAIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAN+nfomB
8SvinoOjLpT8shBiWUJWJhRxGzHd6yz/6O02K9bHtbRdScXLcIUA/TnIdZtKBD2WX4LacNQkFqp+
ZNlXVyORDE6lqDY/3WQg6I2yPGjeCtnJUo3gGUqc6JLgHqDPTemdbtzu3ICYfgYQ43SFM/NNQRbe
BuIn68zkITxsj/x60lPsFwCYLDg+TqjBZSdVTOvjOIrO8+JnVsdnjW9rrpSiubY1Dber/dnWntCg
/CWSZg8BXhdAW8N/etZ8suOTwnKbOTBNOIu2lWDr7JsqtQxViDkBlZCIRnfIfnSoQzNLPpOUnbQM
1HnwoIuT869xK1XNoJV/W9FKI7xSNJXyrOPgstGd6swXcmsMCufinnCXUIBcLP5XNcFXJszY9b
XPOjhFLhRAQUzXjGY72wCMUV8p63g5z0pTHpNCVmJFDR6ionKEtU0zvqAIZndLuoA+wzaUJGss0n
08It4B7E02EVjl/j4/9IlooFu/rGIkjk200cZq8V3vFsUbEivbs/s4quEXMBePOFkOS0mcKM8b+d
cinF/2B5/38Xfz2Zry2w91HzK5F7CovDeVQPz3mOiVH3tfzd+QMZg8qw3pVHub47BjggujPy74C6
BtCTzuitr9ygvscPbtC3sG1ZyZK0I5BbWZkvgfvXcyQoCxNAT2GiuBU4rGyM6cXDJXDo8SAgMBAAGj
ggHZMIIB1TCBxwYDVR0RBIG/MIG8hhVodHRwOi8vd3d3Lml6ZW5wZS5jb22BD2luZm9AaXplbnBl
LmNvbaSBkTCBjjFHMEUGA1UEGw+SVpFTlBFIFMuQS4gLSBDSUYgQTAxMzM3MjYwLVJNZXJjLlZp
dG9yaWEtR2FzdGVpeiBUMTA1NSBGNjIgUzgxQzBBBgNVBAkMOkF2ZGEgZGVsIE1lZGI0ZXIyYW5l
byBFdG9yYmlkZWEgMTQgLSAwMTAxMCBWaXRvcmlhL Udhc3BlaXonDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFKQXHU5I1++HIS5/jrh1yvWL04x9MB8GA1UdIwQYMBaA
FB0cZQ6o8iV7tJHP5LGx5r1VdGwFMDoGA1UdIAQzMDEwLwYEVR0gADAnMCUGCCsGAQUFBwIBFhlo
dHRwOi8vd3d3Lml6ZW5wZS5jb20vY3BzMDcGCCsGAQUFBwEBBCswKTAnBggrBgEFBQcwAYYhaHR0
cDovL29jc3AuaXplbnBlLmNvbTo4MDk0MDMDMGA1UdHwQsMCowKKAmoCSGJmbl0dHA6L y9jcmwuaXpl
bnBlLmNvbS9jZkrYmluI.2FybDIwCwYJKoZIhvcNAQELA4ICAQA3qh2Msr3tOt6Pt1QYuv8ecbx
kHCuxvqnFQSDbp+dRnd5GKJN45emgOkUGKQ6Aq68VSO7060r6PuE0EZKksH9ryRu8x9bSEVSPyge
lC95ITxstkM7M39xc1QHtBxkqyHtooDIY3vySOcbFy0AAo/HfSr8HoJJjIDm/Q5MROKvpTBtOhoq
LkTHe1utfDtrzZsatCiaozmakGgMDSpnpCqI9dL NzdvaXyEbt1gIDIiAjGv4p/ihJyYxJz0LuD/4O
OIQ04qpdvttfoaIIL6BHwoahjaF+5N+/gUlNYVcSDrMOCKBtyg2hmj0lt/LuLnxoL63+D0yAQexCB
al3me3/8YHL7WgWrzpKNmqYh+eak5Vnbm4YMcGtkbhwL1v/UzU/o4gykBTgKerzAIGCIMN42HlvvJ
ELCZiCrNPkuUnGwM1gEiBC5j9ELZzzS33OOuDhCyrDMRUjnz20BmGwJZ4bnLr5D6/1ENsOYWhz
fxVIC666RgZK9vvBQLqTKVduH8u9Lz0p3lcrKRSTfxRrVUc1J5rytX24OkjIMplPohqvjpOZSQt
OoY1GPPgumxOyFHB+7lbc48S5PBYnDSHEqnuYIlz5IPhXURkJkyn1YSdrw2lrB3OORqoOKzYdz
FArY7jwExjRvqXTJUIxJ1HpeCZap+lh1m1pH4kd7hxS/bdhiw==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Izenpe.com*

Issuer O: *IZENPE S.A.*

Issuer C: *ES*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Valid from: *Wed Oct 20 10:16:02 CEST 2010*

Valid to: *Sun Dec 13 00:00:00 CET 2037*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DF:A7:7E:89:81:F3:9B:E2:C2:83:A3:2E:94:FC:B2:10:62:59:42:56:26:14:68:1B:31:DD:EB:2C:FF:E8:ED:19:2B:D6:C
7:AD:B4:5D:49:C5:CB:72:55:00:FD:39:C8:77:6B:4A:F0:3D:96:5F:82:DA:70:D4:31:15:AA:7E:64:D9:57:57:23:91:0C:4E:A5:A8:36:3F:DD:64:20:E8:8D:B2:3C:68:DE:0A:D9:C9:52:8D:E0:19:4A:9E:E8:92:E0:1E:A0:CF:4D:
E9:9D:6E:DC:EE:DC:80:98:7E:06:10:E3:74:85:33:F3:4D:41:16:DE:06:E2:67:EB:CA:E4:21:3C:6C:8F:FC:7A:D2:53:EC:17:00:98:2C:38:3E:4E:A8:C1:65:27:55:4C:EB:E3:3B:5A:CE:F3:E2:67:56:C7:67:8D:6F:6B:AE:94:A2:
B9:B6:35:0D:B7:AB:FD:D9:D6:9E:D0:A0:FC:25:92:66:0F:01:5E:17:40:5B:C3:7F:7A:D6:7C:B2:E3:93:C2:72:9B:39:30:4D:38:8B:B6:95:60:EB:EC:9B:2A:B5:0C:55:88:39:01:95:90:88:46:77:DF:7E:7F:28:43:33:4B:3E:93:94
:35:B4:0C:D4:78:B0:9E:81:2E:4F:C8:BD:C4:AD:57:36:82:55:FD:6F:45:2A:5E:F1:48:D2:57:CA:B3:8F:82:CB:46:77:AB:30:5D:C9:EC:30:2B:9F:9E:77:17:52:50:5C:2C:FF:F9:5C:D7:85:5F:5B:33:62:5F:5B:5C:F3:A3:84:52:E
1:44:04:14:CD:78:C6:63:BD:B0:08:C5:15:F2:9E:B7:83:9C:F4:A5:31:E9:34:25:66:24:50:D1:EA:2A:27:28:4B:54:D3:3B:EA:01:F6:67:74:BB:A8:03:EC:33:69:42:46:B2:CD:27:D3:C2:2D:E0:1E:C4:D3:61:15:8E:5F:E3:E3:FF:
65:96:8A:05:BB:FA:C6:22:48:E4:DB:4D:1C:66:AF:15:DE:F1:6C:51:B1:22:BD:BB:3F:B3:8A:AE:11:73:01:78:F3:85:90:E4:B4:99:C2:8C:F1:BF:9D:72:29:C5:FF:60:79:FF:7F:17:7F:3D:99:AF:2D:B0:F7:51:F3:2B:91:7B:0A:8
B:C3:79:54:0F:AF:79:8E:89:51:F7:B5:FC:DD:F9:03:19:83:CA:B0:DE:95:47:B9:BE:3B:06:3A:A0:BA:33:F2:EF:80:BA:06:20:84:6A:28:ED:AF:DB:E0:BE:C7:8F:68:2D:EC:1B:56:72:64:AD:08:48:16:D6:66:4B:E0:96:F5:DC:
C9:0A:02:C4:D0:13:D8:6B:81:53:8A:C6:C8:CE:9E:5C:32:57:0E:8F:39:02:03:01:00:01

Subject Alternative Name

http://www.izenpe.com

info@izenpe.com

STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints *IsCA: true*

Subject Key Identifier *A4:17:1D:4E:65:D7:EF:87:95:2E:7F:8E:B8:75:CB:05:8B:D3:8C:7D*

Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.izenpe.com/cps

Authority Info Access *http://ocsp.izenpe.com:8094*

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7E:D1:93:61:AD:73:4D:70:3F:BA:DF:02:9F:52:EC:3B:66:48:D8:DD:56:BA:BA:08:84:ED:4F:85:9B:5B:93:75*

X509SubjectName

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-12-21T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.7*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.9*

16.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

16.1.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)*
Name	*[es]*	*Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)*

Service digital identities

X509SubjectName

Subject CN:	*Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)*
Subject OU:	*NZZ Ziurtagiri publikoa - Certificado publico SCI*
Subject O:	*IZENPE S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*pBcdTmXX74eVLn+OuHXLBYvTjH0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

16.1.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.7

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.8

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.9

16.1.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

16.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)

Name [es] Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)

Service digital identities

X509SubjectName

Subject CN: Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)

Subject OU: NZZ Ziurtagiri publikoa - Certificado publico SCI

Subject O: IZENPE S.A.

Subject C: ES

X509SKI

X509 SK I pBcdTmXX74eVLn+OuHXLBYvTjH0=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time *2009-07-17T00:00:00Z*

16.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.7*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.9*

16.2 - Service (granted): Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)*

Name *[es]* *Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *133503482272988939655787341095582449805*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHQzCCBSugAwIBAgIQZG/V3gQ1QzdJo6nRSP5AjTANBgkqhkiG9w0BAQUFADA4MQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMuQSAxEzARBgNVBAMMCklkZW5uZS5jb20wHhcNMDkwMjI0
MDgwMzI5WhcNMzcxMjEyMjMwMDAwWjCBpTELMAkGA1UEBhMCRVMxFDASBgNVBAoMC0laRU5QRSBT
LkEuMTowOAYDVQQLDDFBWlogWml1cnRhZ2lyaSBwdWJsaWtvYSAtIENlcnRpZmlj YWRvIHB1Ymxp
Y28gU0NBMUQwQgYDVQQDDDdFQUVrbyBlQWV0YWtvIGxhbmdpbGVlbiBDQSAtIENBIHBlcnNvbmFs
IGRlIEFBUFAgdmFzYZFzJCgyKTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANXwe264
IBTryz2sVkcKo+TxXbNIuOnMeF1MmOhD5IUcAg16LX1tuZOYz3R6GXONAgzLasaAtPlnp94mmHrzun
po1i8xb+C+2uS+DJN3RNAmf/E7r1VhxTCsKuID7NPhBI1Ep9Luin1w7+2IVKamHcr+UvHJ/kxhwM
dfKLHk9hrEN/yPhAnwB4DHmVA1QyfquGrm0LxDHjggO9fo8iGrE+TS1eMIZtUVZel7BEM2EtctN
AjtR4Nar4HBTACKfSPHw=SUiu7m32kNOtoxW6rN/C3yGnX1g6j8vPS9/nkT4EfgMRJ16JMORfdAY
dyP3pteon/zdRkgxAHxwFFBgG75FpYZT+5jPBKcztzILZ6ymqHBiIl/vycBGazxQ4MufxhOt+cmV1
xccrY9jNGL0yJu4jRgc74zKCBfzo4mZOhlPeOKbaOus7X6pKquVbeFvd5Kg19y0hIoYAvKgyjTd
kfTWUrZrksA8d04J3zwY0WDTxw5CnKLdLdMSbrA7uW8z3XNcNDCMcfwRihCNpfKXwBo/Q+sEjYf
MkEY2e9pGA4ji7Mnrvmwsiv1.qEAXQTFWMk/2ooYhJmfCnDKcDGWsAVvk2UrqHYhQ7sM87yIZPVzw
LES7TU6nmbh0JRSSgN+CSF8DgGRSbNTIW72PVU/+kA3ZfvAYHzgJ9KqgwQV7wc5pzoEvAgMBAAGj
ggHZMIIB1TCBxwYDVR0RBIG/MIG8hhVodHRwOi8vd3d3Lml6ZW5wZS5jb22BD2luZm9AaXplbnBl
LmNvbaSBkTCBjjFHMEUGA1UEC gw+SVpFTlBFIFMuQS4gLSBDSUYgQTAxMzM3MjYwLVJNZXJjLlZp
dG9yaWEtR2FzdGVpeiBUMTA1NSBGNjlgUzgxQzBBBgNVBAkMOkF2ZGEgZGVsIE1lZGI0ZXIyYW5l
byBFdG9yYmlkZWEgMTQgLSAwMTAxMCBWaXRvcmlhL.Udhc3BlaXonDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMavlmhQvm+hSRTcuZ2XPY1z536aMB8GA1UdIwQYMBaA
FB0cZQ6o8iV7tJHP5LGx5r1VdGwFMDoGA1UdIAQzMDEwLwYEVR0gADAnMCUGCCsGAQUFBwIBFhlo
dHRwOi8vd3d3Lml6ZW5wZS5jb20vY3BzMDcGCCsGAQUFBwEBBCswKTAnBggrBgEFBQcwAYYhaHR0
cDovL29jc3AuaXplbnBlLmNvbTo4MDk0MDMDGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly9czmwuaXpl
bnBlLmNvbS9jZXRYmluI.2FybDlwDQYJKoZIhvcNAQEFBQADggIBAGlW+Gd1JbFYeqHoz2fCuzXJ
CnK5vzjo0nvcS53aQGynbXNCHwUVAL6rb Q8hP5IEgdSHm0Yuikkcqe YrTj+w7S3PbF6RpboIp8/
kGAS8fcow+XBEv6DPlJZ3DCCnrp2dFjGSs2te2zbS114CI3rbaeWkuU/4+JPBdwJr7snvk+KREn37
dOUFhxoIs7WXMSQUcx85bpaeQUUIs9PEAC11i1/0lFVGianrAzFBMjYYjzwir/dQQtMDtVIKy3ui+Uz5
qOnlyWxI52cgH78Zsu30uieMt0OuXGYEtcgCgWCkYYSOFOUZwXcFmnrylPw4wwN+qBS0kZrO6K
11MHt9CdyHCQXEXXcK8olXGL8lTlhPav+xvgAWY9APAT3h77jG5s/yhQBdbKBZdzDRpSvNO+l6tP
eWkHl+jl56Z+bmDn4OoqrDlVswgvPTHX48IZqM3D14nQKpdOpoZFrz3xiVHvLRL/v8UORoDs4UM
DluzlR79Io VIdYzQdRN+Z/iE9droo2Ot7lHCzBdjyzlX2+bgS6ghHq5SNH6Wn3rYcOQxWGP5CQR
GiFPjjRXOhXGN35Cel/ccsVBKjY/YYXOChPyLTCxUWwPMo33cCr+11jn1ZlnNw4EpgCSSucNR7dvQ
dSpDVMfO2HJzEN7wAazX5wol4psIUSfvqIktb+xWBmj1RUqKrVvO

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Izenpe.com*

Issuer O: *IZENPE S.A.*

Issuer C: *ES*

Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas (2)*

Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Valid from: *Tue Feb 24 09:03:29 CET 2009*

Valid to: *Sun Dec 13 00:00:00 CET 2037*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D5:F0:7B:6E:B8:20:14:F2:CB:6B:15:91:C2:A8:F9:3B:17:6C:D9:6E:3A:73:1E:17:53:26:3A:10:F9:51:C0:20:D7:A2:D
7:D6:D6:99:39:8C:F7:47:A1:97:38:D0:2A:CC:B6:BC:68:0B:4F:96:7A:7D:E2:69:C7:AF:3B:A7:A6:8D:62:F3:16:FE:0B:ED:AE:4B:E0:C9:37:74:4D:02:67:FF:13:BA:F5:56:1C:53:0A:C2:AE:20:3E:CD:3E:10:65:D4:4A:7D:2E
:E8:A7:D7:0E:FE:D9:F5:4A:6A:61:DC:8B:E5:2F:1C:9F:E4:C6:1C:0C:75:F2:8B:1E:4F:61:AC:43:7F:C8:F8:40:9F:00:78:0C:79:95:03:54:32:7E:AB:86:AE:6D:0B:C4:31:E3:82:03:BD:7E:8F:22:1A:B1:3E:4D:2D:5E:32:56:6D:
51:56:5E:97:B0:44:33:61:2D:89:E7:CD:02:38:91:E0:D6:AB:E0:70:53:00:22:9F:48:F1:F0:F9:25:22:BB:B9:B7:DA:43:4E:B6:8C:56:EA:B3:7F:0B:7C:86:9D:7D:60:EA:3F:2F:3D:2F:7F:9E:44:F8:11:F8:0C:44:9D:7A:24:C3:91:
7D:D0:18:77:23:F7:8E:97:A8:9F:FC:DD:46:48:00:7C:8C:70:10:52:21:1B:BE:45:A5:86:53:FB:98:CF:F0:A7:33:B7:32:4B:67:AC:A6:A8:77:E7:95:4B:F2:70:11:9A:CF:14:38:32:E7:F1:84:EB:7E:72:65:75:C5:C7:2B:63:D8:CD
:18:BD:32:26:EE:23:46:07:3B:E3:32:82:05:FC:E8:E2:66:4E:86:53:DE:38:A6:DA:3A:EB:3B:5F:AA:4A:AA:E5:5B:78:5B:DD:E4:A8:35:F6:2C:B4:84:8A:18:02:F2:A0:CA:34:DD:91:F9:53:59:4A:D9:AE:4B:00:F1:DD:38:27:
7C:F0:63:45:83:4F:1C:39:0A:72:8B:74:B7:4C:49:BA:C0:EE:E5:BC:CF:75:CD:70:D0:C2:31:C7:F0:46:28:42:36:97:CA:5F:00:68:FD:0F:AC:12:36:1F:32:41:18:D9:EF:69:18:0E:23:89:33:27:AE:F9:B0:B2:2B:CB:A8:40:17:41:
31:56:32:4F:F6:A2:86:21:26:67:C2:9C:32:9C:0C:65:AC:01:5B:E4:D9:4A:EA:1D:88:50:EE:C3:3C:EF:29:59:3D:5C:F0:2C:44:BB:D5:4E:A7:99:B8:74:25:14:92:80:DF:82:E4:5F:03:A8:64:52:6C:D4:E5:5B:BD:8F:55:4F:A4:03
:76:5F:BC:06:07:FE:02:7D:FC:AB:A9:C1:05:7B:C1:EE:69:8E:81:2F:02:03:01:00:01
```


Subject Alternative Name

http://www.izenpe.com

info@izenpe.com

STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints *IsCA: true*

Subject Key Identifier *C6:AF:96:68:50:BE:6F:A1:E5:14:DC:B9:9D:97:3D:8D:73:E7:7E:9A*

Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.izenpe.com/cps

Authority Info Access *http://ocsp.izenpe.com:8094*

CRL Distribution Points

http://crl.izenpe.com/cgi-bin/arl2

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

1F:11:A6:55:5C:C6:F2:4D:43:E6:E4:E3:0E:E8:04:D4:16:45:84:7B:7F:D1:56:5A:19:18:63:34:5C:4E:25:6F

Certificate fields details

Version:

3

Serial Number:

139873143337968509637750443090365398999

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHPzCCBSmgAwIBAgIQaTqWZ4PiO99MvqbQ2VQ/1zALBgkqhkiG9w0BAQswODELMAkGA1UEBhMC
RVMxFDASBgNVBAoMC0laRU5QRSBTLkEuMRMwEQYDVQQDDApJemVucGUuY29tMB4XDTEwMTAyMDA4
MjI0MFoXDTM3MT1xMjIzMDAwMFowgaUxCzAJBgNVBAYTAkVTMRQwEgYDVQQKDAtJWkVOUEUgUy5B
LjE6MDgGA1UECwwxQVpaIFppdXI0YWdpcmkgcHVzb6Gtrb2EgLSBDZXI0aWZpY2FkbyBwdWlsaWNv
IFNDQTFEMEIGA1UEAww7RUFFa28gSEFldGFrbyBsYW5naWxlZW4gQ0EgLSBDQSBwZXJzb25hbCBk
ZSBBQVBQIHZhc2NhcyAoMikwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDV8HtuuCAU
8strFZHCqPk7F2zZbjpzHhd1JjoQ+VHAINei19bWm7mM90ehlzjQKsy2vGgL15Z6feJpx687p6aN
YvMW/gvtrkvqyTd01QJn/xOe6VYcUwrCrrA+zT4QZdRK8S7ap9bO3tn1Snph3Iv1Lxyf5MYcDHXy
rx5PYaxID8j4QJ8AeAx5lQNUMn6thq5tCS8Qx44IDvX6PlhqxPk0tXjJWbVFWXpewRDNhLYnnzQI4
keDWq+BwUwAin0jx8PkllruSt9pDTraMVuqzfwt8hp19YOo/Lz0vf55E+BH4DESdeiTDkX3QGHcj
94i6XqJ/83UZIAHyMeBBSIRu+RaWGU/uYzCnM7cyS2esqqh355VL8nARms8UODLn8YTrfnJldcXH
K2PYzRi9Mibud0YHO+MrggX86OJmToZT3jm2jrrO1+qSqrIW3Ib3eSoNiYstISKGALyoMo0ZH5
U1IK2a5LAPHdOCd88GNFg08sOQpyi3S3TEm6wO7lvM91zXDQwjHH8EYoQjaXyl8AaP0PrBI2HzJB
GNnvaRgOI4kzJ675sLIry6hAF0ExVjJP9qKGlSZnwpwynAxlrAFb5NIK6h2IUO7DPO8pWT1c8CxE
u9VOp5m4dCUUkoDIfguRIA6bkUmzUSVu9j1VPpAN2X7wGB/4CfjyrqcEFc8HuaY6BLwIDAQABo4IB
2TCCAdUwgccGA1UdEQSBvzCBvIYVaHR0cDovL3d3dy5pemVucGUuY29tgQ9pbmZvQGl6ZW5wZS5j
b22kgZEwgY4xRzBFBgNVBAoMPkIaRU5QRSBTLkEuIC0gQ0lGIEEwMTMzNzI2MCTSTWVyYy5WaXRv
cmlhLUdhc3RlaXogVDEwNTUgRjYyIFM4MUMwQQYDVQQDDpBdmRhIGRlbCBNZWRpdGVycmFuZW8g
RXRvcmJpZGVhIDE0IC0gMDEwMTAgVml0b3JpYS1HYXN0ZWl6MA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgEGMB0GA1UdDgQWBBTGr5ZoUL5voeUU/3Lmdlz2Nc+d+mjAIBgNVHSMEGDAWgBQd
HGUOqPlle7SRz+SXsea9VXRuBTA6BgNVHSAEMzAxMC8GBFUdIAAwIzAIBggrBgEFBQcCARYZaHR0
cDovL3d3dy5pemVucGUuY29tL2NwczA3BggrBgEFBQcBAQQrMCkwJwYIKwYBBQUHMAGGG2h0dHA6
Ly9vY3NwL ml6ZW5wZS5jb206ODA5NDAzBgNVHR8ELDAqMCigIqAkhiJodHRwOi8vY3JsLml6ZW5w
ZS5jb20vY2dpL WJpbi9hcmwyMAsGCSqGSIb3DQEBCwOCAgEAkx3edUCTBGZHCSn9QcOxTT2OvNLg
mf/7NTbbrPJnQ4FvoowzZ0pflicrubbWIJyEKDAPUnEfa9w9lCCj9OYoOdG75TEw58Kqs1CaezNTZ
JR3YGzH2JRT63IBrhe5hjKyAgWl0YoG0theqQr8ry12sACPe+VJw6MA1/34SZTb3KW/t1Qw8TXSM
64ldDp3spfomG51SkE7mh/DYAxr795PZEDvorEox7/TYd2w3rBx1iXmk4CsuCfYnhitbePBMJMPu
KJOj9Onqvi7cYByMe4W9R8dkgCY760dS8C7ZSXDtNHvCvQmMvRPpsuOW7AuLGAk7zh2Wz8MtOMMM
fBNmFt2UUZxirt2dJL9UkmwhDNdeebdH21OJrza9tmKAMFmsOYCh+MD+lLaWAudy9AwDjM5wv
zYDCIg2UV2DOEpMq+kyIA20s8WmjhsiQ9+QqBETYKtbJ7pGgcFc5R8faSugeM+AsGO0bm4I6mUTaq
UmdxVze8Swl2Tx/hqm1k77+lyowzr274KEMEADm2NHQvubuR8UZPzT4VADeIp6qqeiys7a2+FQCw
6E5eX2Y4qbzEFN6vnBBSzwtOjl5WF/6JdQZj/oPaD61YkAytx+WLl87xlIvtqYsmpsly5w8iZTz0
rm5dr147DuTSL2xZwemFBuhEMPh5DW+IzunqqCzxYCyjpVM=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer CN:

Izenpe.com

Issuer O:

IZENPE S.A.

Issuer C:

ES

Subject CN:

EAEko HAetako langileen CA - CA personal de AAPP vascas (2)

Subject OU:

AZZ Ziurtagiri publikoa - Certificado publico SCA

Subject O:

IZENPE S.A.

Subject C:

ES

Valid from:

Wed Oct 20 10:22:40 CEST 2010

Valid to:

Sun Dec 13 00:00:00 CET 2037

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D5:F0:7B:6E:B8:20:14:F2:CB:6B:15:91:C2:A8:F9:3B:17:6C:D9:6E:3A:73:1E:17:53:26:3A:10:F9:51:C0:20:D7:A2:D
7:D6:D6:99:39:8C:F7:47:A1:97:38:D0:2A:CC:B6:BC:68:0B:4F:96:7A:7D:E2:69:C7:AF:3B:A7:A6:8D:62:F3:16:FE:0B:ED:AE:4B:E0:C9:37:74:4D:02:67:FF:13:BA:F5:56:1C:53:0A:C2:AE:20:3E:CD:3E:10:65:D4:4A:7D:2E
:E8:A7:D7:0E:FE:D9:F5:4A:6A:61:DC:8B:E5:2F:1C:9F:E4:C6:1C:0C:75:F2:8B:1E:4F:61:AC:43:7F:C8:F8:40:9F:00:78:0C:79:95:03:54:32:7E:AB:86:AE:6D:0B:C4:31:E3:82:03:BD:7E:8F:22:1A:B1:3E:4D:2D:5E:32:56:6D:
51:56:5E:97:B0:44:33:61:2D:89:E7:CD:02:38:91:E0:D6:AB:E0:70:53:00:22:9F:48:F1:F0:F9:25:22:BB:B9:B7:DA:43:4E:B6:8C:56:EA:B3:7F:0B:7C:86:9D:7D:60:EA:3F:2F:3D:2F:7F:9E:44:F8:11:F8:0C:44:9D:7A:24:C3:91:
7D:D0:18:77:23:F7:8E:97:A8:9F:FC:DD:46:48:00:7C:8C:70:10:52:21:1B:BE:45:A5:86:53:FB:98:CF:F0:A7:33:B7:32:4B:67:AC:A6:A8:77:E7:95:4B:F2:70:11:9A:CF:14:38:32:E7:F1:84:EB:7E:72:65:75:C5:C7:2B:63:D8:CD
:18:BD:32:26:EE:23:46:07:3B:E3:32:82:05:FC:E8:E2:66:4E:86:53:DE:38:A6:DA:3A:EB:3B:5F:AA:4A:AA:E5:5B:78:5B:DD:E4:A8:35:F6:2C:B4:84:8A:18:02:F2:A0:CA:34:DD:91:F9:53:59:4A:D9:AE:4B:00:F1:DD:38:27:
7C:F0:63:45:83:4F:1C:39:0A:72:8B:74:B7:4C:49:BA:C0:EE:E5:BC:CF:75:CD:70:D0:C2:31:C7:F0:46:28:42:36:97:CA:5F:00:68:FD:0F:AC:12:36:1F:32:41:18:D9:EF:69:18:0E:23:89:33:27:AE:F9:B0:B2:2B:CB:A8:40:17:41:
31:56:32:4F:F6:A2:86:21:26:67:C2:9C:32:9C:0C:65:AC:01:5B:E4:D9:4A:EA:1D:88:50:EE:C3:3C:EF:29:59:3D:5C:F0:2C:44:BB:D5:4E:A7:99:B8:74:25:14:92:80:DF:82:E4:5F:03:A8:64:52:6C:D4:E5:5B:BD:8F:55:4F:A4:03
:76:5F:BC:06:07:FE:02:7D:FC:AB:A9:C1:05:7B:C1:EE:69:8E:81:2F:02:03:01:00:01
```

Subject Alternative Name	*http://www.izenpe.com* *info@izenpe.com* *STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*C6:AF:96:68:50:BE:6F:A1:E5:14:DC:B9:9D:97:3D:8D:73:E7:7E:9A*
Authority Key Identifier	*1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.izenpe.com/cps*
Authority Info Access	*http://ocsp.izenpe.com:8094*
CRL Distribution Points	*http://crl.izenpe.com/cgi-bin/arl2*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*25:30:3C:FD:0B:F1:BA:A1:EF:24:8C:29:F0:73:FF:FC:2E:7C:81:58:2E:E2:3B:45:C7:F1:C3:B3:2E:34:1A:D8*

X509SubjectName

Subject CN:	*EAEko HAetako langileen CA - CA personal de AAPP vascas (2)*
Subject OU:	*AZZ Ziurtagiri publikoa - Certificado publico SCA*
Subject O:	*IZENPE S.A.*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*

	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.14777.4.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.14777.4.4*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.14777.4.5*

16.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.2.3 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)*
Name	*[es]*	*Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)*

Service digital identities

X509SubjectName

Subject CN:	*EAEko HAetako langileen CA - CA personal de AAPP vascas (2)*
Subject OU:	*AZZ Ziurtagiri publikoa - Certificado publico SCA*
Subject O:	*IZENPE S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*xq+WaFC+b6HlFNy5nZc9jXPnfpo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-07-17T00:00:00Z*

16.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.4.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.4.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.4.5*

16.3 - Service (withdrawn): Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

Name *[es]* *Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *12*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGJTCCBQ2gAwIBAgIBDDANBgkqhkiG9w0BAQUFADCB0DELMAkGA1UEBhMCRVMxSDBGBgNVBAoT
P0laRU5QRSBTLkEuIC0gQ0lGIEEtMDEzMzcyNjAtUk1lcmMuVml0b3JpYS1HYXN0ZWl6IFQxMDU1
IEY2MiBTODFCMEAGA1UEBxM5QXZkYSBkZWwgTWVkaXRlcnJhbmVvIEV0b3JiaWRlYSAzIC0gMDEw
MTAgVml0b3JpYS1HYXN0ZWl6MRMwEQYDVQQDEwpJemVucGUuY29tMR4wHAYJKoZIhvcNAQkBFg9J
bmZvQGI6ZW5wZS5jb20wHhcNMDMwMjA0MTc0NjI1WhcNMTMwMjAzMjMwMDAwWjCCATsxCzAJBgNV
BAYTAkVTMUgwRgYDVQQKEz9WkVOUEUgIUy5BL1AtIENJRiBBLTAxMzM3MjYwLVJNZXJjL1ZpdG9y
aWEtR2FzdGVpeiBUMTA1NSBGNjIgUzgxQjBABgNVBAcTOUF2ZGEgZGVslE1lZGl0ZXJyYWSlbyBF
dG9yYmlkZWEgMyAtIDAxMDEwIFZpdG9yaWEtR2FzdGVpejE6MDgGA1UECxMxTlpaIFppdXJ0YWdp
cmkgcHVibGlrb2EgLSBDZX0taWZpY2FkbyBwdWJsaWNvIFNDSTFCMEAGA1UEAxM5SGVvcml0YXIg
ZXRhIEVyYWt1bmRlZW4gQ0lEgLSBDQSBkZSBDaXVkYWRhbm9zIHkgRW50aWRhZGV2aMR4wHAYJKoZI
hvcNAQkBFg9JbmZvQGI6ZW5wZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDb
AGfZvAwm2goSyIUlxIHwR789g8DIpcsXiujsbm3ivLBbyZSyXJrCw1G8T0QKTixfv1I1BEjnbx3y/
HZoyJoTzgTV+PdTBRR6jr/YaJ1vqdrrL70A3scEmezjjSNmgjZjOJa7ppoid+IFNtCoXy/WqypK
FVNfdwxertqvxvgtosms0IDqUsxVOQNtQAk+iu6TfqRkjfDH/PmHuHwC7lW03QowvP617C2lB
DUBF9UVCoyVDXyUlN3htwfm7lKqT9cKIPxwicXelkB6RmThwiFE74GhPmIfr30wSiGegpco/kOq
KK5ZgY6k2xYWCDYxXcqh8h9lSATzsVJBf0z9AgMBAAGjggGaMIIBljAgBgNVHREEGTAXhhVodHRw
Oi8vd3d3Lml6ZW5wZS5jb20wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0O
BBYEFNU9trgnbYQ6qC/UHTNDTTuc225WyMIH9BgNVHSMEgfUwgfKAFQpWT+w8g6EUiHBssFIsAH
QVtCoYHWplHTMlHQMQswCQYDVQQGEwJFUzFIMEYGA1UEChM/SVpFTlBFIFMuQS4gLSBDSUYgQS0w
MTMzNzI2MC1STWVyYy5WaXRvcmlhLUdhc3RlaXogVDEwNTUgRjYyIFM4MUlwQAYDVQQHEzlBdmRh
IGRlbCBNZWRpdGVycmFuZW8gRXRvcmJpZGVhIDMgLSAwMTAxMCBWaXRvcmlhLUdhc3RlaXoxEzAR
BgNVBAMTCXl6ZW5wZS5jb20tHjAcBgkqhkiG9w0BCQEWD0luZm9AaXplbmBlLmNvbYIBATAyBgNV
HR8EKzApMCegJaAjhiFodHRw0i8vd3d3Lml6ZW5wZS5jb20vY2dpLWJpb9hcmwxDQYJKoZIhvcN
AQEFBQADggEBAETEH2yN1hOxbsk4jImqCL6M7HSgPmkVGYzS/oZAEsPemJsNg0z0NMpknrecHjdl
8mVQIkMzYgaCKQsimJXCLxwzz7sQu5bwqgfi5TMXKmrTiV9RpxX2KjjJT6KoTxWptAKRHKbKiq
iRqsSYOrDTazzdyuhKiRgEEcM5oN7cnyc5RHJJOM/VFlDdbKSqDU3C0uzDdZ6b0+0VBoYHema
tHQPBnODKX5Cnk5rkFz9r9RHdou9HLIfZRzbranB6sH2ABcxq6upQlt1BtEFJ18b3hyAtHXSkSA
mwoaHno/DBcFMbCaGNWDJ1GvY1EaHUJ0D1zo7LzcN/pti+D4N3I=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer E: *Info@izenpe.com*

Issuer CN: *Izenpe.com*

Issuer L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Issuer O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Issuer C: *ES*

Subject E: *Info@izenpe.com*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

Valid from: *Tue Feb 04 18:46:25 CET 2003*

Valid to: *Mon Feb 04 00:00:00 CET 2013*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DB:00:67:D9:BC:0C:26:DA:0A:12:C8:85:25:C4:81:F0:47:BF:3D:83:C0:C8:A5:CB:17:8A:E8:EC:6E:6D:E2:BC:B0:5B:C9:94:B2:5C:9A:C2:C3:51:BC:4F:44:0A:4E:2C:5F:BE:5D:41:12:39:DB:C7:7C:BF:1D:9A:32:8E:84:F3:81:35:7E:3D:D4:C1:45:1E:A3:AF:F6:1A:22:3B:EA:76:BA:CB:EF:40:37:B1:C1:26:7B:38:E3:48:D9:A0:8D:98:CE:25:AE:E9:A6:88:9D:F8:81:4D:B6:D0:A8:5F:2F:D6:AA:FA:4A:15:53:5F:77:0C:68:AE:DA:AF:8B:1C:A0:B6:8B:26:B3:47:C3:A9:4B:31:54:E3:8D:8E:D4:00:93:E8:AE:8B:A4:C5:AB:C9:23:7C:31:FF:3E:68:A1:B8:7C:02:ED:6D:37:42:8C:2F:3F:AD:7B:0B:69:41:0D:40:45:E5:45:42:A3:25:43:5F:25:25:37:78:6D:C1:F9:BB:7E:4A:93:F5:C2:9F:3F:1C:22:71:77:A5:90:1E:91:99:38:70:88:51:3B:E0:68:4F:98:87:EB:DF:4C:12:8A:21:9E:82:97:28:FE:43:AA:28:AE:59:81:8E:A4:DB:16:16:08:36:2F:5D:CA:A1:F2:1F:65:48:04:F3:B1:52:41:7F:4C:FD:02:03:01:00:01

Subject Alternative Name *http://www.izenpe.com*

Basic Constraints *IsCA: true*

Subject Key Identifier *D5:3D:B6:B8:27:6D:84:3A:A8:25:07:4C:D0:D3:4E:EB:36:DB:95:B2*

Authority Key Identifier *EA:56:4F:EC:3C:83:A1:14:88:78:81:B2:2B:05:22:C0:07:41:5B:42*

CRL Distribution Points *http://www.izenpe.com/cgi-bin/arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *5C:68:F4:98:B2:38:B3:B2:AD:F8:A7:04:74:CF:24:F6:32:67:58:1B:ED:47:96:9F:B1:8B:5E:1B:4A:AB:80:A9*

X509SubjectName

Subject E: *Info@izenpe.com*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.9*

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.7

16.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

16.3.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)

Name [es] Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)

Service digital identities

X509SubjectName

Subject E: Info@izenpe.com

Subject CN: Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades

Subject OU: NZZ Ziurtagiri publikoa - Certificado publico SCI

Subject L: Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz

Subject O: IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Subject C: ES

X509SKI

X509 SK I 1T22uCdthDqoJQdM0NNO6zbblbI=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased

Status Starting Time 2009-07-17T00:00:00Z

16.3.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.14777.2.9*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.14777.2.7*

16.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*
Name	*[es]*	*Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

Service digital identities

X509SubjectName

Subject E:	*Info@izenpe.com*
Subject CN:	*Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*
Subject OU:	*NZZ Ziurtagiri publikoa - Certificado publico SCI*
Subject L:	*Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*
Subject O:	*IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Subject C:	*ES*

X509SKI

X509 SK I *1T22uCdthDqoJQdM0NNO6zbblbI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2005-03-03T00:00:00Z*

16.3.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.7*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.2.9*

16.4 - Service (withdrawn): Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

Name *[es]* *Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *20*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGIzCCBQugAwIBAgIBFDANBgkqhkiG9w0BAQUFADCB0DELMAkGA1UEBhMCRVMxSDBGBgNVBAoT
P0laRU5QRSBTLkEulC0gQ0lGIEEtMDEzMzcyNjAtUk1lcmMuVml0b3JpYS1HYXN0ZWl6IFQxMDU1
IEY2MiBTODFCMEAGA1UEBxM5QXZkYSBkZWwgTWVkaXRlcnJhbmVvIEV0b3JiaWRlYSAzICOgMDEw
MTAgVml0b3JpYS1HYXN0ZWl6MRMwEQYDVQQDEwpIemVucGUuY29tMR4wHAYJKoZIhvcNAQkBFg9J
bmZvQGl6ZW5wZS5jb20wHhcNMDMwNDA4MTMyNzIxWhcNMTMwNDA3MjIwMDAwWjCCATIxCzAJBgNV
BAYTAkVTMUgwRgYDVQQKEz9JWkVOUEUgUy5BLiAtIENJRiBBLTAxMzM3MjYwLVJNZXJjLlZpdG9y
aWEtR2FzdGVpezBUMTA1NSBGNjIgUzgxQjBABgNVBAcTOUF2ZGEgZGVsIE1lZGl0ZXJyYWSlbyBF
dG9yYmlkZWEgMyAtIDAxMDEwIFZpdG9yaWEtR2FzdGVpejE6MDgGA1UECxMzQVpaIFppdXJ0YWdp
cmkgcHVibGlrb2EgLSBDZXJ0aWZpY2FkbyBwdWJsaWNvIFNDQTFAMD4GA1UEAxM3RUJFa2g8eSEFI
dGFrbyBsYW5naWxlZW4gQ0EgLSBDQSBwZXJzb25hbCBkZSBBQVBQIHZhc2NhczEeMBwGCSqGSIb3
DQEJARYPSW5mb0BpcmVucGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlxWF
U8sG1T7xVCHbIOgRbXYKN3R/HTrzt3tzx3jJl+27jaoPfTVqHKM2NMAOQfzbtH3pODbJS+kg8j
E0V617eFHWh0lOG2WT/F3OF8YEuCxNTD19HVQ2e7oyywb980m2d0dDyqXxZzzSvX+ww3KTgKUw7
N5KXKUK+0QCY9SBKDZVMg/8Ji9rbiVVwizWiPYc3icGn1A9lhuTLXEbLhwwG+zHfjkkIfKa/FRi
Edx4xn8dZurTYSsauIw5E9CwhuAOlo0bmku0QYletNeJvWT3sKnUGO1T8G54jLUQ81mjuNQ+I5UB
Vce/jseP4V/qLGLlNR8gaY04Dhj3eS24vQIDAQABo4IBmjCCAZYwIAYDVR0RBBkwF4YVaHR0cDov
L3d3cfc5pemVucGUuY29tMAMGA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQW
BBSilI+zaOhIbcH7WlabLBRo2CMnyjCB/QYDVR0jBIH1MIHyhgBTqVk/sPIObFlh4gblrBSLAB0Fb
OqGB1qSB0zCB0DELMAkGA1UEBhMCRVMxSDBGBgNVBAoTP0laRU5QRSBTLkEulC0gQ0lGIEEtMDEz
MzcyNjAtUk1lcmMuVml0b3JpYS1HYXN0ZWl6IFQxMDU1IEY2MiBTODFCMEAGA1UEBxM5QXZkYSBk
ZWwgTWVkaXRlcnJhbmVvIEV0b3JiaWRlYSAzICOgMDEwMTAgVml0b3JpYS1HYXN0ZWl6MRMwEQYD
VQQDEwpIemVucGUuY29tMR4wHAYJKoZIhvcNAQkBFg9JbmZvQGl6ZW5wZS5jb22CAQEwMgYDVR0f
BCswKTAnoCWgI4YhaHR0cDovL3d3dy5pemVucGUuY29tL2NnaS1iaW4vYXJsMA0GCSqGSIb3DQEB
BQUAA4IBAQBiQABl3vNMh7MtUOCK1EVlI0STZocgfa7wlob5edykYDLLygwPrwjkPjs3eZHUGlN
VCOfA59ymjheIaQ5JynaH12HTDuDOOs33WVOnH3bJ1du4jpFPsn3WvqRaESb2nOBG6vFcLVVE
0+6dMdnmJnJ8b2EIsCXH5WzcJUOxz4j/GL2mZ5gETV2/xQxYacNl9Ma17etoyHFXHcObGkjSQudC
SVyrM9dcLBY5bO4OAGHQdBdGT/6E0A0cdYciRlC6vtZg0e5wC6EtET4AzX2yRMTGSE+O3PlguUH
IVE+Z3MKXutCuKMVt8ITDcvnjYX1H8moxDQYU0ZtiQG03qtS

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer E: *Info@izenpe.com*

Issuer CN: *Izenpe.com*

Issuer L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Issuer O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Issuer C: *ES*

Subject E: *Info@izenpe.com*

Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas*

Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

Valid from: *Tue Apr 08 15:27:21 CEST 2003*

Valid to: *Mon Apr 08 00:00:00 CEST 2013*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:97:15:85:53:CB:06:4F:B4:F1:54:21:DB:0C:6A:51:6D:76:0A:37:74:7F:1D:F4:EB:CE:DD:ED:CF:1D:E3:DE:5F:B6:EE
:36:A8:3D:F4:DF:56:A1:CA:33:63:4C:00:E4:1F:CD:BB:47:DE:93:83:6C:94:BE:92:0F:23:13:45:7A:D7:B7:85:1D:68:74:94:E1:B6:59:3F:C5:DC:E1:7C:54:4B:82:70:D7:FF:0F:5F:47:55:0D:9E:EE:8F:F2:C1:BF:7C:D2:6D:9D:
D1:D0:F2:A9:7C:59:CF:34:AF:5F:EC:30:DC:A4:E0:29:4C:3B:37:92:97:29:42:BE:D1:00:A3:63:D4:81:28:36:55:32:0F:FC:26:2F:6B:6E:25:53:C2:2C:D6:88:F6:1E:DE:27:06:9F:50:3D:96:1B:93:2D:71:1B:2E:1C:30:1B:EC:C7
:7E:39:24:21:F2:9A:FC:54:62:11:DC:78:C6:7F:1D:66:EA:D3:61:2B:1A:B8:8C:39:13:D0:B0:86:E0:0E:96:8D:1B:9A:4B:B4:41:89:5E:B4:D7:89:BD:67:F7:B0:A9:D4:18:ED:53:F0:6E:78:8C:B5:10:F3:59:A3:B8:D4:3E:23:95:
01:55:E7:BF:8E:C7:8F:E1:5F:EA:2C:62:E5:35:1F:20:69:8D:38:0E:18:F7:79:2D:B8:BD:02:03:01:00:01
```


Subject Alternative Name *http://www.izenpe.com*

Basic Constraints *IsCA: true*

Subject Key Identifier *A2:94:8F:B3:68:E8:5F:6D:C1:FB:5A:56:9B:2C:14:68:D8:23:27:CA*

Authority Key Identifier *EA:56:4F:EC:3C:83:A1:14:88:78:81:B2:2B:05:22:C0:07:41:5B:42*

CRL Distribution Points *http://www.izenpe.com/cgi-bin/arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0A:07:55:F0:F8:78:EB:9C:D3:13:48:8B:6C:79:91:90:C0:4E:59:27:54:16:30:63:83:02:4D:E7:8A:F8:47:38*

X509SubjectName

Subject E: *Info@izenpe.com*

Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas*

Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.4.3*

16.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.4.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*
Name	*[es]*	*Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

Service digital identities

X509SubjectName

Subject E:	*Info@izenpe.com*
Subject CN:	*EAEko HAetako langileen CA - CA personal de AAPP vascas*
Subject OU:	*AZZ Ziurtagiri publikoa - Certificado publico SCA*
Subject L:	*Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*
Subject O:	*IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Subject C:	*ES*

X509SKI

X509 SK I	*opSPs2joX23B+1pWmywUaNgjJ8o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2009-07-17T00:00:00Z*

16.4.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.14777.4.3*

16.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*
Name	*[es]*	*Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

Service digital identities

X509SubjectName

Subject E:	*Info@izenpe.com*
Subject CN:	*EAEko HAetako langileen CA - CA personal de AAPP vascas*
Subject OU:	*AZZ Ziurtagiri publikoa - Certificado publico SCA*
Subject L:	*Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*
Subject O:	*IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Subject C:	*ES*

X509SKI

X509 SK I	*opSPs2joX23B+1pWmywUaNgjJ8o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2005-03-03T00:00:00Z*

16.4.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.14777.4.3*

16.5 - Service (withdrawn): Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Name *[es]* *Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *561247566300106489036210696103855445 48*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGPTCCBCWgAwIBAgIQKjk8JSCZz05Lc99cVI4VZDANBgkqhkiG9w0BAQUFADA4MQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMuQS4xEzARBgNVBAMMCkl6ZW5wZS5jb20wHhcNMTAwMjEx
MTA0MzQwWhcNMjAwMjExMTA0MzQwWjCBnzELMAkGA1UEBhMCRVMxFDASBgNVBAoMC0laRU5QRSBT
LkEuMTIwMAYDVQQLDCJaaXVyaGFnaXJpIHB1Ymxpa29hIC0gQ2VydGlmaWNhZCg6cHVibGlhcFG
MEQGA1UEAww9RXVza28gSmF1cmxhcml0emFrbyBsYW5naWxlZW4gQ0EgLSBDQSBwZXJzb25hbCBH
b2JpZXJubyBWYXNjbzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPkmPWuKUpT91q+
6iK7SSmj2rNRYurT3toL OcljdHQwE9+IL8LqEA90Eiteybwb FZlS9L+PIFLXlRp5TLRJ1VSvyH
SigmR4/SWiDJvaXsR23mj+KaG6tnWvlhhtuFjazBu0N4UjVwoIX72p2cD+igoKNAZJnbwkjtvmj
NJKv0ESg8R2lkCE8zl4b1IwtZ16e6gi786rFmXYgBL7e2yiUzFTjkxmB2i84FzNhv7P6MP7fB8BU
G3m2LwTKZt2qTMhlgNPWMFFp3TsbcOBRwfXD9QyadreYoFhoPX+UvPagtcMDTbtRMmphUrG65HRs
HXHkmjbosNjj1M5Vw4+431MCAwEAAaOCAdkwggHVMIHHBgNVHREgb8wgbyGFWh0dHA6Ly93d3cu
aXplbnBlLmNvbYEPpW5mb0BpemVucGUuY29tgiRMdGOMUcwRQYDVQQKDD5JWkVOUEUgIy5BLiAt
IENlRiBBMDEzMzcyNjAtUk1lcmMuVm0b3pYS1HYXN0ZW16IFQxMDU1IEY2MtBTODFDMEEGA1UE
CQw6QXZkYSBkZWwgTWVkaXRlcnJhbmVvIEV0b3JiaWRlYSAxNCAtIDAxMDEwIFZpdG9yaWEtR2Fz
dGVpcjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQU8aMeVYzVopte
fPpWxldq5wAdugwHwYDVR0jBBgwFoAUHRxlDgjyJXu0kc/ksbHmvVV0bAUwOgYDVR0gBIDMwMTAv
BgRVHSAAMCcwJQYIKwYBBQUHAgEWGWh0dIA6L y93d3cuaXplbnBlLmNvbS9jcHMwNwYIKwYBBQUH
AQEEKzApMCcGCCsGAQUFBzABhhtodHRwOi8vb2NzcC5pemVucGUuY29tOjgwOTQwMwYDVR0fBCww
KjAooCagJIYiaHR0cDovL2NybC5pemVucGUuY29tL2NnaS1aW4vYXJsMjANBgkqhkiG9w0BAQUF
AAOCAgEAXt0gTg5gLqC7Y1ha/rYNONnZ0MK2aDOehzX5NjIT3xRF4jCS/7ooF2UhlhO1ajxP0fZb
KUh+gEBFSnE9C4hxA9YQPfQb6zlWKO3cmrusvIWgtM7jZVYor5snAKrE4hv7yG22uVOslVXza0xy
Tj3gUDxf3AaDWHYoqE7Q7W3fr36qN+uyEC+MWMOSZRZJ7RpdN1hnj1Umu14vUlb0q2sVp/sN7lPu
Pt+ZngkWnB9a1fyYKqzQc1eTcaJTbzlBfinrjXZhNKZR6ZekzI6gCqgBLk/VuRZMUxyVJgwPTzWaf
PZ+VytuSS1lhM2Igt3s3Fqm5dc6zwUHLhd9L1BDWTtmZrH6QU7ZcSGDLL3vJ8+AWmtrUiZSbyZuK
1wkayGm9bmc2KdapVtFCy1gfsCSBEnbVUxcopnatlgeoBXNAdbmLmCj8jONCCazK743n3ZMmgNk7PJ
HfDqjLJZdHZcR/CCsbNdp7JaYSI1pHx68kOjwtSCagOOmCtL2enSKiY35PFSEY1XVR9BcijgflVR
9JnhbksGQ0kulkwuWchUvw/mNlUlgghur8KpZWawN8NT9AqcDlHBi8nR+GE6287hdrwzuOB+kx6W
BpBCfndMcaFIWATXRsStt6Vo8UKG1rp7jtQe49smXCRMiavCzvfNVwltZGkygFsPUq4Il5CQr4zx
54/biy0=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN:	*Izenpe.com*
Issuer O:	*IZENPE S.A.*
Issuer C:	*ES*
Subject CN:	*Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*
Subject OU:	*Ziurtagiri publikoa - Certificado publico*
Subject O:	*IZENPE S.A.*
Subject C:	*ES*
Valid from:	*Thu Feb 11 11:43:40 CET 2010*
Valid to:	*Tue Feb 11 11:43:40 CET 2020*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B3:E4:98:F5:AE:29:4A:53:F7:5A:BE:EA:22:BB:49:29:A3:DA:B3:51:62:EA:FF:23:7B:68:2C:E7:25:8D:D1:D0:C0:4F:7E:20:BF:0B:A8:40:3D:D0:48:AD:7B:26:F0:6C:56:65:E6:2F:4B:F8:F2:05:2D:79:51:A7:9D:4B:44:9D:55:4A:FC:87:E6:28:26:47:8F:D2:5A:D0:C9:C1:7C:51:DB:79:A3:F8:AA:86:B7:D9:D6:BC:88:5B:7E:E1:48:8D:AC:C1:BB:43:78:52:35:70:A0:85:FB:DA:9D:9E:0F:E8:E0:A0:A3:40:66:59:DB:C2:48:ED:CA:BA:63:36:52:AF:D0:44:A0:F1:1D:A5:90:21:3C:CC:8E:1B:D4:8C:2D:64:8E:9E:EA:08:BB:F3:AA:C5:99:76:20:04:BE:DE:DB:28:94:CC:54:E3:93:19:81:DA:2F:38:17:33:61:BF:B3:FA:30:FE:DF:07:C0:54:1B:79:B6:2F:04:CA:66:DD:AA:4C:C8:65:80:D3:D6:30:51:69:DD:3B:1B:70:E0:51:C1:F5:C3:F5:0C:9A:76:B7:98:A0:58:68:3D:7F:94:BC:F6:A0:B5:C3:03:4D:BB:51:32:6A:61:52:B1:BA:E4:74:6C:1D:71:E4:9A:36:E8:B0:D8:E3:D4:CE:55:C3:8F:B8:DF:53:02:03:01:00:01*
Subject Alternative Name	*http://www.izenpe.com* *info@izenpe.com* *STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*F1:A3:1E:55:8C:D5:A2:9B:5E:7C:5A:56:C4:87:6A:E7:00:1D:B9:A8*
Authority Key Identifier	*1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.izenpe.com/cps*
Authority Info Access	*http://ocsp.izenpe.com:8094*
CRL Distribution Points	*http://crl.izenpe.com/cgi-bin/arl2*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*0B:C3:6A:9B:6E:42:DD:BF:07:4C:FE:38:83:4F:20:0C:D4:4C:1D:28:E2:35:29:CF:E6:29:BC:48:4B:98:98:B9*

X509SubjectName

Subject CN:	*Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*
Subject OU:	*Ziurtagiri publikoa - Certificado publico*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2018-03-15T01:00:00Z*

Scheme Service Definition URI

URI [en] *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI [es] *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.5.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Name [es] *Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Service digital identities

X509SubjectName

Subject CN: *Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Subject OU: *Ziurtagiri publikoa - Certificado publico*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *8aMeVYzVoptefFpWxIdq5wAduag=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

16.5.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.5.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Name *[es]* *Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Service digital identities

X509SubjectName

Subject CN: *Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Subject OU: *Ziurtagiri publikoa - Certificado publico*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *8aMeVYzVoptefFpWxIdq5wAduag=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-07-30T00:00:00Z*

16.6 - Service (granted): Qualified timestamps issued by tsa.izenpe.com

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified timestamps issued by tsa.izenpe.com*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por tsa.izenpe.com*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *153937334957709364140310094114160524157*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHyDCCBbCgAwIBAgIQc89Alm7KoeNYmE4j9Ko7tTANBgkqhkiG9w0BAQsFADA4MQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMufQS4xEzARBgNVBAMMCklzZW5wZS5jb20wHhcNMTcwMjA2
MTAyMTIzWhcNMjIwMjA2MTAyMTIzWjBWMQswCQYDVQQGEwJFUzEUMBIGA1UECgwLSVpFTlBFIFMu
QS4xGDAWBgNVBGEMD1ZBVEVTLUEwMTMzNzI2MDEXMBUGA1UEAwwOdHNhLml6ZW5wZS5jb20wggli
MA0GCSqGSIb3DQEBAQUAAA4ICDwAwggIKAoICAQCJp1wLCY3z0yIWNQlbJjATWB9IyyegVATH0pM
ANjd3LBvIf9aJVocgBmZ0yaAM4Uz29k3bAiK/hwB2KUKmZufhuLwK89PS1Vq/T3k7pzaRWMAcqs
Nbt3D+L4HIoEt2MuBmRurs5U+6hakTQkzw4P+1NDiXY0Lv4h7lZ8Qf87ssr1R+7YNF5F10BW/aMC
hOsxa0pgtceTyifc6U/AkEtkNY6TI/Wt1m8ahyeBDqKId7BBC/DOpL/5q22sn0JXjyrXBlVUdSx9I
Bbll7miLqxyDqEAirER6Kp7lRVMM8t+sKKILUcT6k4VySKkTmHpO93tws26lllgcz5BMdNg81Sq2D
CQSpI3igsbvzANgYhX79QT1RzukYsiDAMlheI/87IGqBF/R1/dT6DCmubI7q4G+ZVNPKWFV5R/bKEy
V0mXSsDDf9zzS7ZXmRTAgnp7q6GIT5GHB30UXnadic0WywvTmF2VAsHGgUi5TiWpJZG2KobGFWIM
6xhnC7Rl9vn1GceIYgfAGHyF2V0lnflICO4viZRYQ2tq5sBxjvAOhE6h2F5Wa2O/V1M7IV52MVhG
HgUjw7Gl87UYByKUABXCsAMzLYa/4BtVFeLNdZkJbGuZVEMG5cdem7IYuFc25SwZxcDSb9LeDYQa
Xq2rA7YMpmg8yR/+0jvIpvdRzapMXDtW8pnlQIDAQABo4ICrzCCAqowghAGA1UdEgSBqDCBpYEP
aWSnb0BpemVucGUuY29pIGRMIGOMUcwRQYDVQQKDD5IWkVOUEUgUy5BLAtIENJRiBBMDEzMzcy
NjAtUk1lcmMuVml0b3JpYS1HYXN0ZW16IFQxMDU1IEY2MiBTODFDMEEGA1UECQw6QXZkYSBkZWwg
TWVkaXRlcnJhbmVvIEV0b3JiaWRlYSAxNCAtIDAxMDEwIFZpdG9yaWEtR2FzdGVpcjAOBgNVHQ8B
Af8EBAMCB4AwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFOHaTOpL9BbMn53Iz0G
mvyFgeI2MB8GA1UdIwQYMBaAFB0kZQ6o86V7tHP5LGx5r1VdGwFMDcGCCsGAQUFBwEBCswKTAn
BggrBgEFBQcwA4YbaHR0cDovL3RzYS5pemVucGUuY29tOjgwOTMvMIIBHQYDVR0gBIIBFDCCARAw
ggEMBgkrBgEEAIM5AwMwgf4wJQYIKwYBBQUHAgEWGWh0dHA6Ly93d3cuaXplbnBlLmNvbS9jcHMw
gdQGCCsGAQUFBwICMIHHGoHEQmVybWVlbiBtdWdhayBlemFndXR6ZWtvIHd3dy5pemVucGUuY29t
IFppdXJ0YWdpcmlhbiBrb25maWFudIpbIGli6YW4gYXVvcmVlaWsga29udHJhdHVhIGlyYW1cnJp
LkxpbW10YWNpb25lcyBkZSBnYXJhbnRpYXMgZW4gd3d3Lml6ZW5wZS5jb20gQ29uc3VsdGUgZWwg
Y29udHJhdG8gYW50ZXMgZGUgY29uZmlhciBlbiBlbCBjZXJ0aWZpY2FkbzAzBgNVHR8ELDAqMCig
JqAkhJodHRwOi8vY3JsLml6ZW5wZS5jb20vY2dpL.WJpbi9hcmwyMA0GCSqGSIb3DQEBCwUAA4IC
AQBqJcHprXlHOCBJwWuEABCj16SA7zQLvNnB/5azLMp6fxfutBt8xhNHTozZBQsqpa8E0UB+x0Ca
tdcrs3TsQAadD/cTNmbyR7mR8IM4WyUwdMLPRRRJyIO3nWIfKgpmqdknmQkusSXc9u4b1rxm
1pS34nXtC/DEBcrtPubTqzGQq5mw7kuU+rE+gYLFSX+rCAqG8+SdA0Cegv2KxvEWeFunzebU/krcN
qhEDkYVtNhRD39df+k+3vrmybr1ubZ76Rl2NHmq4tn0Pcqa3+17+ggoQ2L1YWWZw/vqTXxiZI47S
UcK47BTKUQjO16SGu3s3hKW9g3AIEpEoayR1/j9zoQPO9er3Ku8J9Rp+39WmjwO5CmiPA3L2mFd+
vbrea1gKWsdwtv6p7gBlmlq1IJeIfMWck91SQtsNOYSPpsPY/btUQ9LLqz+AoJeYDELJhpOjesJr
4iGGbOFytkUNKE7bT6ZMkFBI01lLyB1XIs7Uv/UtTnOKhoCjq922VEv99kT9BjecHDbDCrba37yj3
xOXZyTZ8dCCkOlhjOX2vjQ4vvt31HSa46eVMds+6bLUDnGn9KC6aTp+2hcv37tM/gtXjE//VNuFH
l4F18pea3qg7vGkWCHLPMYE7fy4LhJZdFCGt9QCChn5ogt6I2mF3diKbAD8IOhpKQKI6GJpCyq6R
Kg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Izenpe.com*

Issuer O: *IZENPE S.A.*

Issuer C: *ES*

Subject CN: *tsa.izenpe.com*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Valid from: *Mon Feb 06 11:21:23 CET 2017*

Valid to: *Sun Feb 06 11:21:23 CET 2022*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A5:DA:9D:70:2C:26:37:CF:4C:A5:58:D4:1F:6C:98:C0:4D:60:7D:23:2C:9E:81:50:13:1F:4A:4C:00:DA:E3:77:72:C1:
BC:7F:5A:25:5A:1C:80:19:99:D3:26:80:33:85:2B:DB:DB:37:84:08:8A:FE:1C:01:D8:A5:0A:99:9B:9F:86:E2:F0:2B:CF:4F:4A:2D:55:AB:F4:F7:93:BA:73:69:15:8C:01:CA:AC:35:B2:37:0F:E2:F8:1C:8A:04:D9:F3:2E:06:64:
6E:AE:CE:54:FB:A8:5A:91:34:24:CF:0E:0F:FB:53:43:89:76:34:2E:FE:21:EC:86:61:41:F4:BB:A2:CA:F5:47:EE:D8:34:5E:45:97:40:56:FD:A3:02:84:EB:31:6B:4A:60:B5:C7:93:CA:37:DC:E9:40:24:12:D9:0D:63:A4:E5:FD:6
B:75:9B:C6:A1:C9:E0:43:A8:A9:5D:EC:10:42:FC:33:A9:2F:FE:6A:DB:6B:27:D0:95:E3:CA:B5:C1:95:55:1D:4B:1F:48:05:B9:48:EE:68:8B:AB:1C:83:A8:40:22:AC:44:7A:2A:9E:C8:45:53:0C:F2:DF:AC:28:A2:0B:51:C4:F
A:93:85:72:48:A9:13:98:7A:4E:F7:7B:70:B3:6E:A5:96:58:33:E4:13:1D:36:0F:35:4A:AD:83:09:04:A9:97:78:A0:B1:BB:F3:00:D8:18:85:7E:FD:41:32:51:C6:46:2C:88:30:0C:96:17:88:FF:CE:C8:1A:A0:45:FD:15:1D:4F:A0:C
2:9A:E6:E5:EE:AE:06:F9:95:4D:3C:A5:85:57:94:7F:6C:A1:32:57:49:97:E6:C0:DF:27:DC:F3:4B:B6:57:99:17:C0:82:7A:7B:AB:A1:88:4F:91:87:07:7D:14:5E:76:9D:89:CD:16:CB:04:E6:17:65:40:B0:71:A0:52:2E:7F:4E:25:
A9:25:91:B6:2A:88:46:15:67:CC:EB:18:67:0B:B4:65:F6:F9:F5:19:C7:88:62:07:C0:18:7C:85:D9:5D:08:AE:17:C8:08:EE:2F:89:94:58:43:6B:6A:E6:C0:71:8E:F0:0E:84:4E:A1:D8:5E:56:6B:63:BF:57:53:3B:7D:5E:76:31:58:4
6:1E:05:23:C3:B1:A5:F3:B5:18:07:22:94:00:15:C2:B0:03:33:2D:86:BF:E0:1B:55:15:E2:CD:75:99:09:6C:6B:99:54:43:06:E5:C7:5E:9B:B2:18:B8:57:36:E5:2C:19:CD:C0:D2:6F:D2:DE:0D:84:1A:5E:AD:AB:03:B6:0C:A6:68:
3C:C9:1F:FE:D2:3B:C8:A6:F7:51:CD:AA:4C:5C:3B:56:F2:99:E7:95:02:03:01:00:01

Issuer Alternative Name	*info@izenpe.com*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*E7:C7:69:33:A9:2F:D0:61:32:7E:77:23:3D:06:9F:0C:85:81:E1:76*
Authority Key Identifier	*1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.14777.3.3* *CPS pointer: http://www.izenpe.com/cps* *CPS text: [Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri.Limitaciones de garantias en www.izenpe.com Consulte el contrato antes de confiar en el certificado]*
CRL Distribution Points	*http://crl.izenpe.com/cgi-bin/arl2*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*CD:77:0A:3B:A5:00:5B:AC:3F:6E:F2:9E:7F:A4:C7:BE:A1:EF:41:BE:52:12:53:56:DA:0D:D1:8F:04:5C:92:19*

X509SubjectName

Subject CN:	*tsa.izenpe.com*
Subject 2.5.4.97:	*VATES-A01337260*
Subject O:	*IZENPE S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*58dpM6kv0GEyfncjPQafDIWB4XY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-07-21T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.7 - Service (granted): Qualified certificates issued by CA de certificados SSL EV

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by CA de certificados SSL EV*

Name *[es]* *Certificados cualificados emitidos por CA de certificados SSL EV*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *145477172158191020923658859389206702465*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHFjCCBQCgAwIBAgIQbXHrW3u2tjZMvqhl46SpgTALBgkqhkiG9w0BAQswODELMAkGA1UEBhMC
RVMxFDASBgNVBAoMC0laR1i5QRSBTLkEuMRMwEQYDVQQDDApJemVucGUuY29tMB4XDTEwMTAyMDA4
Mjg1NloXDTIwMTAyMDA4MjgINlowgYExCzAJBgNVBAYTAkVTMRQwEgYDVQQKDAtJWkYOUlEIgUy5B
LjE4MDYGA1UECwwvQlogWml1cnRhZ2lyaSBwdWJsaWtvYSAtIENlcnRpZmlj YWRvIHB1YmxpY28g
RVYxIjAgBgNVBAMMGUNBIGRlIENlcnRpZmlj YWRvcyBTU0wgRVYwggIiMA0GCSqGSIb3DQEBAQUA
A4ICDwAwggIKAoICAQDrsp1NSv8Un9VoFovUEmCabq7yhqgSWTR6x3N6hvSywo491fK+t09Y9FB
0jsj8S/azt/TKd7S0U0mlv7DTYv2bSIBpfoah2VSbLuYHy9OBbMDHtpSNGBHMc+ds4TV/dsH4x9Fi
wH9FddFDXtuVXaUpQpQVtusYwgkn6zUx5OH7KBgNoo7GC7Vt+MAcLrNxIkMuKjKVkQtZagX+zcJB
stVXwVvJrOGPidnrG523Iu4QN9KvdNCOAUtON4F1U1eS6CdGeuDUrQuibCYTPWk7en+wk57Yqjik
jg2DYXWj19k8WTXj9AxAizXpZgXgv7F/RyDl+Yt+DqsPFVH76HD529wU9zQ2zY+cky49eGG/HAGg
fXFezKUsEJt0M54N9tnCUDFSlAJh67T0tAIfleVdyougUhtPseDfj6mPfc23icHpJMcRrtPtY1K4uV
266hkt99jgEhEbU3/DbMQ6OkJ8xoIoDMbLMHBKBy8kj1tTFBt6Ca1dGH+7+ngJKIsM50plWbzZu81
4l2YoVgEtNJcvCmWdY8AvIULDO6IoGs0j4ldLQmphY/R/7VKFda/S8Xg52NY67N+HQdPTbmpNxYq
cJMM4iC/OnODWv+FSdBFo8gbzJIV3pdFOKCeYEX1QopHiBQucaBajFtzN4gmj7YZ6lLQw6WV0JBD
r5hQDDzvctHYUjP2xQIDAQABo4IB1DCCAdAwgccGA1UdEQSBvzCBvIYVaHR0cDovL3d3dy5pemVu
cGUuY29tgQ9pbmZvQGI6ZW5wZS5jb22kgZEwgY4xRzBFBgNVBAoMPklaRUSQRSBTLkEuIC0gQ0IG
IEEwMTMzNzI2MC1STWVyYy5WaXRvcmlhLUdhc3RlaXogVDEwNTUgRjYyIFM4MUMwQQYDVQQJDDpB
dmRhIGRlbCBNZWRpdGVycmFuZW8gRXRvcmJpZGVhIDE0IC0gMDEwMTAgVml0b3JpYS1HYXN0ZWl6
MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSmzmlpLqYhNTs6zwrx
LjBVrBmQIzABgNVHSMEGDAWgBQdHGUOqPIlc7SRz+Sxsea9VXRsBTA6BgNVHSAEMzAxMC8GBFUd
IAAwJzAlBggrBgEFBQcCARYZaHR0cDovL3d3dy5pemVucGUuY29tL2NwczAyBggrBgEFBQcBAQQm
MCQwIgYIKwYBBQUHMAGGFmh0dHA6Ly9vY3NwLmI6ZW5wZS5jb20wMwYDVR0fBCwwKjAooCagJIYi
aHR0cDovL2NybC5pemVucGUuY29tL2NnaS1ia W4vYXJsMjALBgkqhkiG9w0BAQsDggIBAFZbnUyn
MHy160SmISeI7e9v53+gpvCbszYB+TrCQmFRcqhP8dsj7T7ymqOEIJajFEIIkmybyVwgfaqZxw
r+Sc4owsuTkNtlh8tzTO6VYUbTWqPBEFkA0FeiG94N+36b7iUj4OrJK7W9vsGBZq7KIEL y0ExQVG
d5wTi4mV42LRNQyL4qw1sZ+aDVPNVqYpFkWKv1rULQtNwEcWXsg3sn/AmwQeEiRfcSqho5Ab+zh2
TQQngxv0/jH/w1jz1LwzMgR326b7uYwQmvsdkGzIF730xOjBrd8pqUfinUuUGwbzhpLXaTUlOiCh
z34dHcN2k77X/Ib1w0EeZ8ldzbOrd4XnVkgznAbmxPnHV0Lisqdf-4gMtbyJGZOhgSOp0pxdKII
BU13Adw6jwGHylcI10nd0tG04BW0L7Pu8zuPndCp6yEVQDxXXdaECVGaSmVcyb816U4hgwvLeAcC
+jNmQPbgVWVqM5dzrLZPMIawdLwPWcon5pV77s10Rcjs+H1ycfgMzmlkZFKvvYRYGBIwH+WjLOb6
6Vmh2SH414mCbF3itFXZ82IJwsr95cbv87G2hx+2pl0AL8M5I7gpVWk3Plm5pYZua4pnbbWHPX1
JiKlwFu7iHz5+DLrLExocXSogiO+EcR4Gc6j9t0vDV8MK7uVw0Lp/OGzZy/+g1XDaqd

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Izenpe.com*

Issuer O: *IZENPE S.A.*

Issuer C: *ES*

Subject CN: *CA de Certificados SSL EV*

Subject OU: *BZ Ziurtagiri publikoa - Certificado publico EV*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Valid from: *Wed Oct 20 10:28:56 CEST 2010*

Valid to: *Tue Oct 20 10:28:56 CEST 2020*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EB:B2:9D:4D:4A:FF:14:9F:D5:68:16:8B:D4:12:60:9A:6E:AE:F2:86:A8:12:59:34:7A:C7:73:7A:87:FB:D2:CB:0A:38:F7:57:CA:FA:DD:3D:63:D1:41:D2:3B:3F:8F:C4:BF:6B:3B:7F:4C:A7:7B:48:E5:34:9A:5B:D3:0D:35:76:85:22:01:A7:A6:A1:D9:54:A1:52:E6:07:CB:D3:81:6C:C0:C7:B6:9E:4D:18:11:CC:C7:E7:62:E1:35:7F:76:C1:F8:C7:D1:6D:C0:7F:45:75:D1:43:5E:DB:95:5D:A5:29:42:94:15:B6:EB:18:C2:09:27:EB:35:31:E4:E1:FB:28:18:0D:A2:8E:C6:0B:B5:6D:F8:C0:1C:2E:B3:71:22:43:2E:2A:32:95:91:07:D9:6A:05:FE:CD:C2:41:B2:D5:57:C1:5B:C9:AC:E1:8F:89:D9:EB:1B:9D:B7:22:EE:10:37:D2:AF:74:D0:8E:01:4B:4E:37:81:75:53:57:92:E8:27:46:7A:E0:D4:AD:0B:A2:6C:26:13:3D:69:3B:7A:7F:B0:93:9E:D8:AA:38:A4:8A:0D:83:61:75:A3:D7:D9:3C:59:35:E3:F4:0C:40:8B:35:E9:66:05:E0:BF:B1:7F:47:20:C8:F9:8B:7E:0E:AB:0F:15:51:FB:E8:70:F9:DB:DC:14:F7:34:36:CD:8F:9C:93:2E:3D:78:61:BF:1C:01:A0:85:71:5E:AC:A5:28:10:9D:0C:E7:83:7D:B6:70:94:0C:54:88:02:1E:BB:4F:48:80:7F:4B:15:77:2A:2E:81:48:6D:3F:17:83:7E:3E:A6:3E:5A:F6:DF:F8:9C:1E:92:4C:71:1A:DF:3D:F6:35:2B:8B:95:DB:AE:A1:92:DF:5F:80:48:44:6D:4D:FF:0D:B3:10:E8:E9:09:F3:1A:25:A0:33:1B:2C:C1:C1:28:1C:BC:92:3D:6D:4C:50:6D:E8:26:B5:74:61:FE:EF:E9:E0:24:A2:3C:33:9D:29:21:66:F3:66:EF:35:E0:8D:98:A1:58:04:B4:D2:5C:BC:29:96:75:8F:00:BC:85:0B:0C:EE:88:A0:6B:34:8F:82:1D:2D:09:A9:85:8F:D1:FF:B5:4A:15:D6:BF:4B:C5:E0:E7:63:58:EB:B3:7E:21:074F:4D:B9:A9:37:16:2A:70:93:0C:E2:D0:BF:3A:73:83:5A:FF:85:49:D0:45:A3:C8:1B:CC:92:15:DE:97:45:38:A0:9E:60:45:F5:42:8A:47:88:14:2E:71:A0:5A:8C:3B:73:37:88:26:8F:B6:19:E9:F2:D0:C3:A5:95:D0:90:43:AF:98:50:0C:3C:EF:72:D1:D8:52:33:F6:C5:02:03:01:00:01

Subject Alternative Name

http://www.izenpe.com

info@izenpe.com

STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints *IsCA: true*

Subject Key Identifier *A6:CE:69:69:2E:A6:21:35:3B:3A:CF:0A:F1:2E:3F:15:AC:19:90:27*

Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.izenpe.com/cps

Authority Info Access *http://ocsp.izenpe.com*

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B0:8C:19:6A:2E:D1:E8:4F:98:92:DB:1B:61:21:9C:EB:64:28:82:47:8F:39:B0:87:19:60:3D:07:35:FA:03:D1*

X509SubjectName

Subject CN: *CA de Certificados SSL EV*

Subject OU: *BZ Ziurtagiri publikoa - Certificado publico EV*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *ps5paS6mITU7Os8K8S4/FawZkCc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-03-15T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

16.8 - Service (granted): Qualified certificates issued by CA de certificados SSL EV (new)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by CA de certificados SSL EV (new)*
Name	*[es]*	*Certificados cualificados emitidos por CA de certificados SSL EV (nueva)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *138892462179354702629058714957455292581*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHGjCCBQKgAwIBAgIQaH23FxdE2iNbP2Jac5P4pTANBgkqhkiG9w0BAQsFADA4MQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMuQS4xEzARBgNVBAMMCkl6ZW5wZS5jb20wHhcNMTgwNzA2
MTIzNjQxWhcNMjgwNzA2MTIzNjQxWjCBgTELMAkGA1UEBhMCRVMxFDASBgNVBAoMC0laRU5QRSBT
LkEuMTgwNgYDVQQLDC9CWiBaaXVydGFnaXJpIHB1Ymxpa29hICQgQ2VydGlmaWNhZG8gcHVibGlj
byBFVjEiMCAGA1UEAwwZQ0EgZGUgQ2VydGlmaWNhZG9zIFNTTCBFVjCCAiIwDQYJKoZIhvcNAQEB
BQADggIPADCCAgoCggIBAN1INsruuFEV4Z9tcfhNC9neg6vTQYhJPNFJQmKGJVcELjn3Scl8kP0j
JJOWlDKxYiP1dXjzV0FpK2coIXDaV7gHXD912VoPVLmbRyK3UyV5YYTOTGd84ErKtIceYLa7Hv38
zsZnlkL+rtS98QoxvMcZfnjRoLYJ3UZ9l/7j+DX/MdkJ5u6cXRe1vB8tc9FwdWSwTkkLK4+lOhFOW0
o5LDnt99Hs8ds48KEflIbS7qYZty/WySH6pvoi2ZqEAFL4eMlos4TMfVSPdrd13HAB45Il/kdva
0dq6GHfpy3absBZhsxVbmvdAc1f66Ytr/qoLKSwBxRM/cCpQumbS74HVgA2xBPEHM75J/YBa5uM
gI/yx1zoEiaGhExhTMUGG+9od8oqhXzDR1ecyxXqpdVzf4RJB+zgd4LWnVXM3DJC0WBgmFESU/cn0
fqoyb09RPN5vFtjY/HcAuzm39p1RDzlejAWWoQuDA1frKUsk62zWKpJnR3m/WhLo9upz+oW08hA
oILdxH7BOFPL+OOOsWJ8qqQPZpiZQZkwVl2WBaxYufwMgtB4amyPrtRguyIxFmUJxxTI6faL5
XngYkZK1f4Ns2hOfn1qKZEX2C9Ul/CpBrSVQtQMkM0Q3fnYOa7TBDB/P9yroxmrLmXUuG3VOCZ3rt
N70DvcL7KbwiNIX0ld1RAgMBAAGjggHUMIIB0DCBxwYDVR0RBIG/MIG8hhVodHRwOi8vd3d3Lml6
ZW5wZS5jb22BDZluZm9AaXplbnBlLmNvbaSBkTCBjjFHMEUGA1UECgw+SVpFTlBFIFMuQS4gLSBD
SUYgQTAxMzM3MjYwLVJNZXJtLlZpdG9yaWEtR2FzdGVpezBUMTA1NSBGNjlgU2gxQzBBBgNVBAkM
OkF2ZGEgZGVsIE1lZGl0ZXJyYW5lbyBFdG9yYmlkZWEgMTQgLSAwMTAxMCBWaXRvcmlhLUdhc3Rl
aXowDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMbt/nf7UVZN/KvV
47EME6O/VOObMB8GA1UdIwQYMBaAFB0cZQo6o8V7tJHP5LGx5r1VdGwFMDoGA1UdLAQzMDEwLwYE
VR0gADAnMCUGCCsGAQUFBwIBHhodHRwOi8vd3d3Lml6ZW5wZS5jb20vYBBzMDIGCCsGAQUFBwEB
BCYwJDAiBggrBgEFBQcwAYYWaHR0cDovL29jc3AuaXplbnBlLmNvbTAzBgNVHR8ELDAqMCgqJqAk
hiJodHRwOi8vY3JsLml6ZW5wZS5jb20vY2dpLWJpbi9hcmwyMA0GCSqGSIb3DQEBCwUAA4ICAQBY
RlIC3xiMdbPZIP7j+5HtHt1sCFGWfUF8PdWR5CGQHXq9gybOYNDYBg8fQNlI3wKMZCT7WoXn+8e
3eUUzKDlhzU+0f9CNc2bPHIW4mCn8nakJAcy3ZvDFO9C6fK00anu/a1gLDXmR71crRx1vTOu30K2
Lq9sJNzc8DeJWKmXY4VuJ6C5AgwRsmtRIIBhudOyKTeXU72dRDEFejt8bGOt3gIuSEgrlPGEIP1L
RnVVyAnRRWfMOvDjwS5DQQs1j9/YIKS/w9pGB40QsCzUBsHd3N6VCTi59ZDXky0DrA1c1aeQtyX
c90PfgYTwwEwYnQHsR6U0gk8SUB6xSn1nwUuWmHrJtmQGpbGwdax76sEJXNk7XU3ecIyKFCUK8g
X6fYMb/l0hu2O93sEyrGJF9uIcqvduqEjRWQY36F/xOdr/ZIJndVrJ4vMIYN0Xiz/fPS61b3kkrWU
VsknKfic8cuBiqGgop1nt0RNyIpVI49U5sROm3Cfdcf1fdwVA6poiiYQtINhWb6mF0P7+DcfccC3l
lMYvxsfrx+11jl8YCQY18FF65FxPCt+YEBO2hnOnPMK3cA8YvuSol1lkE/StcpcjPeRrvuPy/I+a
t2pj8hv8f4FWMX6Gj8zt8+AoAprvXcQRaiEO4FL5alTv1Rqkv7i0HCGIpc+Ct2ApdcBtC4uSTA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Izenpe.com*

Issuer O:	*IZENPE S.A.*
Issuer C:	*ES*
Subject CN:	*CA de Certificados SSL EV*
Subject OU:	*BZ Ziurtagiri publikoa - Certificado publico EV*
Subject O:	*IZENPE S.A.*
Subject C:	*ES*
Valid from:	*Fri Jul 06 14:36:41 CEST 2018*
Valid to:	*Thu Jul 06 14:36:41 CEST 2028*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DD:48:36:CA:EE:B8:51:15:E1:9F:6D:71:F8:4D:0B:D9:DE:83:AB:D3:41:88:49:3C:D1:49:42:62:86:25:57:04:2E:39:F7:49:C7:FC:90:FD:23:24:93:96:94:32:B1:62:23:F5:75:78:F3:57:41:69:2B:67:28:95:70:DA:57:B8:07:5C:3F:75:D9:5A:0F:54:B9:9B:47:22:B7:53:25:79:61:84:CE:4C:67:7C:E0:4A:CA:B4:87:1E:60:B6:BB:1E:FD:FC:CE:C6:67:22:42:FE:AD:F4:BD:F1:0A:22:BC:C7:19:86:98:D1:A0:B6:37:21:46:7D:53:B8:FE:0D:7F:CC:92:42:79:BB:A7:17:45:ED:6F:07:CC:7D:17:07:56:4B:04:E4:90:B2:B8:FA:53:A1:14:E5:B4:A3:92:C3:9E:DF:7D:1E:CF:1D:76:2E:3C:28:47:E5:21:B4:BB:A9:86:6D:CB:F5:B2:48:7E:A9:BE:88:B6:66:A1:00:14:BE:1E:30:8A:2C:E1:33:1F:57:93:DD:AD:DD:77:1C:00:78:E4:89:7F:91:DB:DA:D1:DA:BA:18:77:E9:CB:76:9B:B0:16:61:B3:15:5B:9A:F7:40:73:57:FA:E9:8B:6B:FE:AA:0B:29:2C:01:C5:13:3F:70:2A:50:BA:B9:DB:4B:BE:07:56:00:36:C4:13:C4:1C:CE:F9:27:F6:01:6B:9B:8C:80:8F:F2:C5:3C:E8:12:26:86:84:4C:61:4C:C5:06:1B:EF:68:77:CA:2A:85:7C:C3:47:57:9C:CB:15:EA:9D:D5:73:7F:84:49:07:EC:E0:77:82:D6:9D:55:CC:DC:32:42:D1:60:60:98:51:12:51:C9:F4:7E:AA:32:6F:4F:51:3C:DE:6F:16:D8:D8:FC:77:80:BB:39:B7:F6:9D:51:0D:C9:5E:8C:05:96:9D:06:83:00:72:6B:29:4B:24:EB:6C:D6:2A:92:63:B9:1D:E6:FD:68:4B:A3:DB:A9:CF:EA:16:3B:C8:40:A1:F2:C8:77:11:FB:04:E1:4F:2F:E3:8E:3A:C5:89:F2:AA:90:3D:9A:48:65:06:64:C1:5D:36:58:16:B1:62:E7:F0:32:38:1F:B7:86:A7:C8:FA:DF:46:0B:A3:C8:8C:45:99:42:71:C5:39:7A:7D:A2:F9:5E:78:18:91:92:B5:7F:83:6C:DA:13:9F:9F:5A:8A:64:45:F6:0B:D5:25:0A:90:6B:49:54:22:40:C9:0C:D1:0D:DF:9D:83:9A:ED:30:43:07:F7:FD:CA:BA:31:9A:B2:E6:5D:4B:86:DD:53:82:67:7A:ED:37:BD:03:BD:C2:FB:29:BC:22:36:55:F4:95:DD:51:02:03:01:00:01*
Subject Alternative Name	*http://www.izenpe.com* *info@izenpe.com* *STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*C6:ED:FE:77:FB:51:56:4D:FC:AB:D5:E3:B1:0C:13:A3:BF:54:E3:9B*
Authority Key Identifier	*1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.izenpe.com/cps*
Authority Info Access	*http://ocsp.izenpe.com*
CRL Distribution Points	*http://crl.izenpe.com/cgi-bin/arl2*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*DB:47:63:39:CC:BF:CC:9E:4B:D1:D6:CB:60:6C:A2:7F:00:67:9E:1E:F8:A5:81:E7:23:63:09:B9:D6:3F:FE:37*

X509SubjectName

Subject CN:	*CA de Certificados SSL EV*
Subject OU:	*BZ Ziurtagiri publikoa - Certificado publico EV*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *xu3+d/tRVk38q9XjsQwTo79U45s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2019-07-15T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI [es] *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

16.9 - Service (granted): Qualified Certificates issued by SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA*

Name [es] *Certificados cualificados de firma y de sello expedidos por SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number:

102715244214283384748977364794814947 71

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGqTCCBJGgAwIBAgIQB7o5QNlyeehfazGZ68988zANBgkqhkiG9w0BAQsFADA/MQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMuQS4xGjAYBgNVBAMMEVJPT1QgQ0EgUUMgSVpFTlBFMB4X
DTIwMDkyMzExMjkyOVoXDTQ1MDkyMzEwNTcxOFowgYcxCzAJBgNVBAYTAkVTMRQwEgYDVQQKDAtJ
WkVOUEUgLUy5BLjEYMBYGA1UEYQwPVkFURVMtQTAxMzM3MjYwMUjgwRgYDVQQDDD9TVUJDQSBRQyBJ
WkVOUEUgLSBBREEJTkTVFJBWklPTFBVQkxJS09BLUFETUJOSVNU/UkFDSU9OIFBVQkxJQ0Ewggli
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCukx3GgwC11P797+WrzqeSXofvR2dQeguo+T
p50cFXcjkgWp4WQC8j0dYh3/2pJ5GlWsOlnRtwZZUap4E74UeKhDkHxhF28mGy9jellopEZFFG3
5cvs9MVslw9hbZ8kK5jiD8X9uzbK/vZdwxLR3lo3BUbx07w0lF+Mg4zTElpk1uVRZYFHpwkHHqN
pQmfpvLVAIQMr8W8OVRydonsxZF+/ID876GvzoNyOrBsd6G1vQDdIKjSDDvup4oZNJc+xCJiLyeD
WRDhFQ9nozPw0mW76MK5x+RL0VG8duaoWLCR5bXDEIsJukPxQ36GDECNObGrCtr0vHRHXckIigl
A3gFWHmw4d6HjyzbiRlIDT358OwZHk3YNKrKvve71HPKB15mfkSMi1WiZG2nV2h34R3CH0hzJF
1Py/ElH/RKwuEpkoH7PmKUJbdjXeBzVj0EVKb1qzr7cq1wzmyn5QRJa8ovHCBPPyOMB070bcFgnn
uq0VRegYy0aYQvFn8juVYd22HlZAEkqntWPMP6bCcwUExZfpIY7eiYjKCOMeGWdKgzBMOPWVVeR
LXJz7jzb+WuCu80FvEGZhJVygTb7puRiASsUdu0hK6cCvx2LkICyPXYemmhnb1O0HYG1PscD0kZt
WX9mqATWb7jltaxdO8j0RusFE7QUdZa0cy8Hcw1DAQABo4IBVjCCAVIwHwYDVR0jBBgwFoAUqWg1
woCxpdS6UiEVFxvYm+OGhpcwHQYDVR0OBBYEFNPh0AAQ5DfbIMBuzZL1nH8Kay5AMDsGA1UdIAQ0
MDIwMAYEVR0gADAoMCYGCCsGAQUFBwIBFhpodHRwczovL3d3dy5pemVucGUuZXVzL2NwczzB2Bggr
BgEFBQcBAQRqMGgwZgYIKwYBBQUIHMAKGWmhddIA6Ly92d5cuaXplbnBlLmVlcy9jb250ZW5pZG9z
L2luZm9ybWFjaW9uL2Nhc19pemVucGUvZXNtY2FzL2FkanVudG9zL0laRUSQRV9ST09UX1FDLmNy
dDASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjA3BgNVHR8EMDAuMCygKqAohiZo
dHRwOi8vY3JsLml6ZW5wZS5ldXMvY2dpL Wpbi9penJvb3RxYzANBgkqhkiG9w0BAQsFAAOCAgEA
dD0tpHnbKe7HqHcPcE2p6dutUP83Lz72Cqlf.lhdnGbeyuaflUPaXMJ4puQnC4EIGR5SXsZcWBzD
2qeKHjdPwvPREFU5+9Y0luLplEWdl/YyAfQmnVygR/K9SSfUW19UpCfiwA+ZuD23O0B5431yyS+Ty
vwLop2nlhKiCE47jxDnG9++yYJnSn1vXqsXmlcnO86jzvVkf8VEQf7E04/4EPwO/YMmrOjzzUN4QX
9RsYg+rp+49cA1N1YMAocjLhsCuDAnuYV54tgJpQ/pFpSZbkLzog4CCHAf0g6nmaDbsOGR8TP7h9
ytEphMrdiKFvvE5HekIfo77wLulmax6Qk1rCq4QKk74WoxjxGWEj2bJpPMe+LpYSBmPMKWck4Wz
wEeKtuQ7IbFoKkizukIVTPKs51PzLGqtqUHBhYgax1Jc4KjT/MrA8dfcombQr5UQLTtZD5YI1
L51BNLJ3iF4LqMe7oS0VNzxs4SJpLc7pz0pGQV+Z8OcJ7B3vceRyUwY68+L+ArtVjJgmHU6sxjlx
YNXHDY2nBu5WwV4f1lIRFXCPtOz4Y4Ot2qdPggobMbzEnI3fJqfwN820e5w8y1pSQDTV8unv7vcK
Etr90ayA6TvdWUkieEhOs+e6jM7CyQ2er/o+oaAcBcFpvJU/Giqr8YzvLWyKJ3UWXUy81TE8et94=

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

ROOT CA QC IZENPE

Issuer O:

IZENPE S.A.

Issuer C:

ES

Subject CN:

SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA

Subject 2.5.4.97:

VATES-A01337260

Subject O:

IZENPE S.A.

Subject C:

ES

Valid from:

Wed Sep 23 13:29:29 CEST 2020

Valid to:

Sat Sep 23 12:57:18 CEST 2045

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AE:93:1D:C6:83:00:B5:D4:FE:FD:EF:DF:96:AF:3A:9E:49:7A:1F:BD:1D:A2:75:07:A0:BA:8F:93:A7:9D:1C:15:77:2 3:92:98:16:A7:85:90:0B:C8:F4:75:88:77:FF:6A:49:E4:69:56:B0:E9:67:46:BC:19:65:46:A9:E0:4E:F8:51:E2:A1:0E:41:F1:84:5D:BC:98:6C:BD:8D:E2:25:A2:91:19:14:51:B7:E5:CB:EC:F4:C5:6C:97:0F:61:6D:9F:24:2B:98:E2 :0F:C5:FD:BB:36:CA:FE:F6:5D:C3:12:D1:DE:5A:37:06:52:5B:C7:4E:F0:D2:51:7E:32:0E:33:4C:42:29:93:5B:95:45:96:05:1E:9C:24:1C:7A:8D:A5:09:9F:A6:F2:D5:00:84:0C:AF:C5:BC:39:54:72:76:89:EC:C5:92:3E:FC:80:F C:EF:A1:AF:CE:83:72:3A:B0:6C:77:A1:B5:BD:00:DD:20:A8:D2:0C:3B:EE:A7:8A:19:34:97:3E:C4:22:62:2F:27:83:59:10:E1:15:0F:67:A3:33:F0:D2:65:BB:E8:C9:39:C7:E4:4B:D1:58:B7:F1:DB:9A:A1:62:C2:47:98:57:0C:4 9:6C:26:E9:0F:C5:0D:FA:18:31:02:34:E8:46:AC:28:AB:D2:F1:D1:1D:77:24:22:28:25:03:78:05:58:79:B0:E1:DE:87:8F:2C:DB:89:19:65:0D:3D:F9:F0:EC:19:1E:4D:D8:34:AA:CA:BE:F7:BB:D4:73:CA:07:5E:6B:9D:F9:12:3 2:2D:56:89:91:B6:9D:5D:A1:DF:84:77:08:7D:0E:87:32:45:D4:FC:BF:12:51:FF:44:AC:2E:12:99:28:1F:B3:E6:29:42:5B:76:35:DE:07:35:63:D0:45:4A:6F:5A:B3:AF:B7:2A:D7:0C:E7:CA:7E:50:44:96:BC:A2:F1:C2:04:F3:F2: 38:C0:74:EF:46:DC:16:09:E7:BA:AD:15:45:E8:18:CB:46:98:42:F1:67:F2:3B:95:61:DD:B6:1E:52:59:00:49:2A:9D:F5:8F:30:FE:9B:09:CC:14:13:16:5F:A6:56:3B:7A:26:23:28:23:8C:78:65:9D:2A:0C:C1:30:E3:D6:55:57:91:2 D:72:73:EE:3C:DB:F9:6B:86:77:41:6F:10:66:61:25:5C:9E:4E:1E:E9:B9:18:A2:01:2B:14:76:ED:21:2B:A7:02:BF:1D:8B:90:90:B2:3D:76:1E:9A:78:67:87:53:B4:1D:8E:B5:3E:C7:03:EA:46:6D:59:7F:66:A8:04:D6:87:B8:C8: B5:AC:5D:3B:C8:F4:46:EB:05:13:B4:14:75:96:B4:73:2F:07:73:02:03:01:00:01

Authority Key Identifier

A9:68:35:C2:80:B1:A5:D4:BA:52:21:15:17:1B:D8:9B:E3:86:86:97

Subject Key Identifier

D3:E1:D0:00:10:E4:37:DB:20:C0:6E:CD:92:F5:9C:7F:0A:6B:2E:40

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.izenpe.eus/cps

Authority Info Access

http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://crl.izenpe.eus/cgi-bin/izrootqc

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm: *SHA-256*

Thumbprint: *1A:48:85:AC:77:F5:55:9B:29:BF:AE:13:C4:86:FF:09:31:21:FA:C2:68:A8:EC:BB:2B:AB:30:3F:5D:A9:42:F9*

X509SubjectName

Subject CN: *SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *0+HQABDkN9sgwG7NkvWcfwprLkA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-04-21T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

16.10 - Service (granted): Qualified certificates issued by SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

Name *[es]* *Certificados cualificados de firma y sello expedidos por SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *451192634252818487577517577191338671 94*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGqDCCBJC2gAwIBAgIQIfGnb9EyDqIfazFpq9XMujANBgkqhkiG9w0BAQsFADA/MQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMuQS4xGjAYBgNVBAMMEVJPT1QgQ0EgUUMgSVpFTlBFMB4X
DTIwMDkyMzExMjg0MVoXDTQ1MDkyMzEwNTcxOFowgYYxCzAJBgNVBAYTAkVTMRQwEgYDVQQKDAtJ
WkVOUEUgUy5BLjE:YMBYGA1UEYQwPVkFURVMtQTAxMzM3MjYwMUcwRQYDVQQDDD5TVUJDQSBRQyBJ
WkVOUEUgLSBlRVJSSVRBUlJlBSyBFVEEgRU5QUkVTQS1DSVVEQURBTklBIFkgRU1JQUkVTQTCCAi1w
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALIGPEPXHSGD3j5WSF4FUzKnG2amk5dpk6wCcaZw
YN6Uewb9W/kBlPsJ7hearXH0rq4n7M/JGqSdfWUw2DtC1MI+7OSHsGtm0fCWyy4I3dOcEqYwiasA
YXfS/ogM8EGReZq9p7ydrKb+bCQym+a8lqLR6G0D07ybIOHN+U2/P5/kH7H92mWFhlPyyIL fpMTZ
Ver4HKGeWxvMNK2bgEAjdC2gapsaJytN6pYZbxjWagyrY0JakqMOGLcB6C/DdlXRjsgRFHjUxwB
hfoDu/uY9Q6jxmO39kAOfyv9zzIDWGJf2oc8wQnomYrPpgGyVEuh/ZGR3CCQcKRw17gsxtWg3x
G4A7qehC9HvIH1z5rpJHWYp2vrcl1ikiAQDib1qK0a+keZfk1xWxAnSHGbhJPXvrScGeJDUF+xcn
ZgGlPDFc/0Mr03kjoxDGRh3xXYS+ICuA3ZS0wwt0XON94X7RejXhCB1z0aGzGpSIu4cVAAI9hFgE
x2rT39KRscmIfzxRNLrSszm4qn2PzYim45iiEiSHAFV+yxpGAIvwCtsoIBMV5UWpBHNd+A/MUzGp
TUxh4X+ghzJbgJSjFWz34DbFk7Q5Mc4qIwkJBBSPvTY18dUxXce+WYJxNAL/LeQ6PZSOxh36T5
pgUVzaj6irLjXh1EkTqEfUj5Bpmt27IGr9X9AgMBAAOjggFWMIIBUjAfBgNVHSMEGDAWgBSpaDXC
gLGi1LpSIRUXG9ib44aGlzAdBgNVHQ4EFgQUYarIL4Lkj7HWPFDTAaBECkbeGqQwOwYDVR0gBDQw
MjAwBgRVHSAAMCgwJgYIKwYBBQUHAgEWGmh0dHBzOi8vd3d3Lml6ZW5wZS5ldXMvY3BzMHYGCCsG
AQUFBwEBBGowaDBmBggrBgEFBQcwAoZaaHR0cDovL3d3dy5pemVucGUuZXYuL2NvbnRlbmlkb3Mv
aW5mb3JtYWNpb24vY2FzX2lbZW5wZS9lc19jYXMvYWRqdW50b3MvSVpFTlBFX1JPT1RfUUMuY3U0
MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMDcGA1UdHwQwMC4wLKAqoCiGJmh0
dHA6Ly9jcmwuaXplbnBlLmV1cy9jZ2ktYmluL2l6cm9vdHFjMA0GCSqGSIb3DQEBCwUAA4ICAQAO
0jeH40zaSwD/Iut0RrjbQoWRWAglcj5p36Tq4OnJ98+y3+cw83A2SCtjwe+m0lt3QVP8+VVNrhvC3
5P1zn4JDEi2FalarRCUlJqO3MJzp1Z1ZbnGQQ7C78D9pWvzZRZX8uLX6OkjWOunC1GirbL7j3DK
sIntGWYksCMVcnhWA532arY+DlRe6D3Y8Ey+5B1CDPz3svWHx29C02LNkpwgVyUwLKxAjicUbp9I
QppScVdY/eG0As+Cs/Ki1WVsGMXmqorYgevbZfQfuBUErXT15MFvcRpzIVZv0HnZhc0KPDhXU+w
jn+/oM4MIqsIo88BzCRbNc2kwq5DwedIAbDFFX4R6cyS65S7RkwRMOHOgz7Fxa5Da+GHAAe2LIf
+qNQyX3RY6cMnhut04B0xow8he/NKZq8u1ZL6QIuOSAPMP9zeSK6Bu0DrUurnNwkqamRKCIIJNGR
eLYtsIwEE1hTwIaARhzcM0eyiglaLgkhU8N8VnetTTA5pbvMfCMITTi/V+8deyzFWwtZshERdiTo
+/UgV74YA0l8sbYPLi63daCqu0hVfWWVNJIc1m553jcAKAO/5VpGSupnuoBJ8H0IYXuQka1xVCLN
+qGlrT57uMqm/01sKtKVGbPwXg0BGCD9bIrvzs2jDW1W9ooPn3uKk+yilfupG2Wm5JvdT2E3OQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ROOT CA QC IZENPE*

Issuer O: *IZENPE S.A.*

Issuer C: *ES*

Subject CN: *SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Valid from: *Wed Sep 23 13:28:41 CEST 2020*

Valid to: *Sat Sep 23 12:57:18 CEST 2045*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B9:46:3C:43:D7:1D:21:83:DE:34:96:48:5E:05:53:32:A7:1B:66:A6:93:97:69:93:AC:02:71:A6:70:60:DE:94:7B:06:FD:5B:F9:01:94:FB:09:EE:17:9A:AD:71:F4:AE:AE:27:EC:CF:C9:1A:A4:9D:7D:65:30:D8:38:82:D4:C2:3E:EC:E4:87:B0:6B:66:D1:F0:96:CB:2E:08:DD:D3:9C:12:A6:30:89:AB:00:61:77:D2:FE:88:0C:F0:41:91:79:9A:BD:A7:BC:9D:AC:A6:FE:6C:24:32:9B:E6:BC:96:A2:D1:E8:6D:03:D3:BC:9B:20:E1:CD:F9:4D:BF:3F:9F:E4:1F:B1:FD:DA:65:85:86:53:F2:C8:82:DF:A4:C4:D9:55:EA:F8:1C:A1:9E:5B:1B:CC:34:AD:9B:80:40:23:74:2D:A0:6A:98:AC:68:9C:AD:37:AA:58:65:BC:63:59:A8:32:AD:8D:09:6A:4A:8C:38:62:DC:07:A0:BF:0D:D2:17:46:3B:20:44:51:E3:53:1C:01:85:FA:03:B8:9C:18:F5:0E:A3:C6:78:8E:DF:D9:00:3A:5C:AF:F7:3C:DF:0D:61:89:7F:6A:1E:07:04:29:A2:66:2B:3E:98:06:C9:51:2E:26:DF:D9:19:1D:C2:09:07:8A:47:0D:7B:82:CC:6D:5A:0D:F1:1B:80:3B:A9:E8:42:F4:7B:DF:1F:5C:F9:AE:92:47:59:8A:76:BE:B7:25:D6:29:22:01:00:E2:6F:5A:8A:D1:AF:A4:79:97:E4:D7:15:B1:02:74:87:19:B8:49:3D:7B:EB:49:C1:9E:24:35:05:FB:17:27:66:01:A5:3C:31:5C:FF:43:2B:D3:79:23:A3:10:C6:46:1D:F1:5D:84:BE:20:2B:80:DD:9F:34:C3:0B:74:5C:E3:7D:E1:7E:D1:7A:35:E1:08:1D:73:D1:A1:B3:1A:94:88:BB:87:15:00:02:3D:84:58:04:C7:6A:D3:DF:D2:91:B1:C9:88:7F:3C:51:34:BA:D2:B3:39:B8:AA:7D:8F:CD:88:A6:E3:98:A2:12:24:87:00:55:7E:CB:1A:46:00:8B:F0:0A:DB:28:20:13:15:E5:45:A9:04:73:5D:F8:0F:CC:53:31:A9:4D:4C:61:E1:7F:AA:86:B2:61:A8:94:A3:15:6C:F7:E0:36:C5:93:B4:39:7C:C7:38:AA:5C:0A:25:F0:52:3E:F4:D8:D7:C7:54:C5:77:9E:F9:66:09:C5:F3:40:2F:F2:DE:43:A3:D9:48:EB:1B:DF:A4:F9:A6:05:15:CD:A8:FA:8A:B2:E3:5E:1D:44:91:3A:84:7D:48:F9:06:99:AD:DB:B2:06:AF:D5:FD:02:03:01:00:01

Authority Key Identifier

A9:68:35:C2:80:B1:A5:D4:BA:52:21:15:17:1B:D8:9B:E3:86:86:97

Subject Key Identifier

61:AA:C8:2F:82:E4:8F:B1:D6:3C:50:D3:01:A0:44:0A:46:DE:1A:A4

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.izenpe.eus/cps

Authority Info Access

http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://crl.izenpe.eus/cgi-bin/izrootqc

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

5C:29:9D:31:59:49:42:41:38:14:5E:5E:E1:DA:67:7D:93:4F:09:5D:8A:5B:F7:86:C7:AB:B8:CB:4F:C6:D6:5A

X509SubjectName

Subject CN:

SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA

Subject 2.5.4.97:

VATES-A01337260

Subject O:

IZENPE S.A.

Subject C:

ES

X509SKI

X509 SK I

YarIL4Lkj7HWPFDTAaBECkbeGqQ=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-04-21T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

16.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.10.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

16.11 - Service (granted): Qualified TimeStamp issued by SUBCA QC IZENPE - TSA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en]	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified TimeStamp issued by SUBCA QC IZENPE - TSA*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por SUBCA QC IZENPE-TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *289043149259703123053355478536087334 63*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHsTCCBZmgAwIBAgIQFb7EwJjBvmNfnBsJTqJLFzANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQG
EwJFUzEUMBIGA1UECgwLSVpFTlBFIFMuQS4xGDAWBgNVBGEMD1ZBVEVTLUEwMTMzNzI2MDEeMBwG
A1UEAwwVU1VCQ0EgUUMgSVpFTlBFIC0gVFNBMB4XDTIwMTAzMDEzNTQxNloXDTI1MTAzMDEzNTQx
NlowVjELMAkGA1UEBhMCRVMxFDASBgNVBAoMC0IaR1SQRSB1TLkEuMRgwFgYDVQRhDA9WQVRFUy1B
MDEzMzcyNjAxFzAVBgNVBAMMDnRz1SSpemVucGUuY29hMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAyDsYtF0sg61SkDg4G7kjy0lgH9W3E5L1izquTp6Gb5xudP910ANsLRr342rEj5gK
QUa8pUg7DU1rjFTjJtUqRvNgakQ6+W07zv53H99Zw4fn5hziJZdwId5pyGatcCoO/7XCtgZVAFzn
A9wI8BRjepXT3AfgXHerFIULBb15KhJoAU+MHwnEthZp3mi5zVrxaYYU9j6Hh9uSV5kXHjIURUs4
PwUbfvWggzXVpbssAwSr+fGvVIpt4CPvhE3W73ycf6Vt0Nih0quRs1uxAvZDaeI7cXSSmYZ5Ib4r
BX2r5H+5qNgYBK736cII9djeeSJS/Db4vkitblamAxftUFrf1Ot52QDO3CFHNJDAcWbOCRnDV5K8T
vgzh2lQNL/OuJ3uxUopyNhw5CKsVGD/81pA6RAfPnYzKgjdd1hlIt1991CAGSJWUA4JM2O2XLAXW
0q2R3ngMWLiSzlGzEXcXiALBrFb47fYg4GUF48Nqa/1Kt+nxs9eyI3wyHS1BELB8I\sBwAsVRpPmK
kz6KsmVOOAGf46fyDublgOmWPEOdNpOw+YZx6R6524ygcjZSIangmzRlcWtNT7mMzefZKzCZxO
67XtAo+rp37ufOZSsgZQK+8TcsrRh6PdZ7heqCyXHyVO3Gbz53ACBuVeCCA+FqCGTCoNSCxVD0
P3j1uj+RkDsCAwEAAaOCAnIwggJuMA4GA1UdDwEB/wQEAwIHgDAWBgNVHSUBAf8EDDAKBggrBgEF
BQcDCDAdBgNVHQ4EFgQUbnlDD9mea3pa1o7uHEjW+87cwwHwYDVR0jBBgwFoAU6oRFun9cSfsV
C6MPDo2c5D=rosEwggEeBgNVHSAEggEVMIIBETCCAQ0GCSsGAQQB8zkKATCB/zAIBggrBgEFBQcC
ARYZaHR0cDovL3dJdy5pemVucGUuZXVzL2NwczCBIQYIKwYBBQUHAgIwgcMgcVLb250c3VsdGEg
d3d3Lml6ZW5wZS5ldXMtZW4gYmFsZGludHphayBldGEga29uZGl6aW9hayB6aXVydGFnaXJpYW4g
ZmlkYXR1IGVkbyBlcmFiaWxpIGF1cnJldGIrIC0gQ29uc3VsdGUgZW4gd3d3Lml6ZW5wZS5ldXMg
bG9zIHTDqXJtaW5vcyBSIGNvbmRpY2lvbmVzIGFiadGVzIGRlIFVoWxpemFyIG8gY29uZmlhcuBl
biBlbCBjZXJ0aWZpY2FkbzAyBggrBgEFBQcBCwQmMCQwIgYIKwYBBQUHMAOGFmhtdHA6Ly90c2Eu
aXplbnBlLmV1cy8wdAYIKwYBBQUHAQEaDBmMGQGCCsGAQUFBzAChlhodHRwOi8vd3d3Lml6ZW5w
ZS5ldXMvY29udGVuaWRvcy9pbmZvcm1hY2lvbi9YXNfaXplbnBlL2VzX2Nhcy9hZGp1bnRvcy9T
VUIDQV9RQ19UU0EuY3J0MDgGA1UdHwQxMC8wLaAroCmGJ2h0dHA6Ly9jcmwuaXplbnBlLmV1cy9j
Z2kzY1mluL2l6ZW5wZVRTQTANBgkqhkiG9w0BAQsFAAOCAgEAVXSns6Sgh31GIkYgZYYmdCbtDWA
/EDoyI5jIT8xJVVLndVldj12wqC3xcYgAArgQK8H84U9RKJUHsq2x66fplAV2vMRoepqAe2S9zGc
aXhkcw5mNgXQF1pWqVadnuSazUiDAZdJmNnPaefVnlj/gY04c/yxHcVf7IOTnhtMxTayFrlpmN/3
x2BUc05UWmAPw+W+6A1NYBbyuQOt5OpvRUlbOmv+fG3ed/8fdcrSOTBJSA2eny9XeDTs5E9O8Tt
jZ2Wk5PzLwIJpbDLOyKMKlkmtcvuz+EmlD2ZtOySnR+IWFBwZkANIELpgcOIrBQnyMPkqjFTA9
F91yVM6Dv3dNAFfPCnA/KF3Oa/4+e2PjTtwOTTEbPGFwDPtz+sHBm3RhW1LFGn4+eOmlyhg+iC7x
32EmWT2Xb0Qa0wmGfyYJFtIFdgo5EK4VVEytGi+dPfnLA5uEjGbTovo/Zhc12/2d5nW1KqPfueC
LxU9OKZ/8Ua7WehazRtm75h0iowGBS15z5vwtqbv6n4UN0W4/XZfrepKSTeGMnuZICvMDoc01LqX
5OVC0LUrwqJRpKvC0Z+2wa2YpYaC+k3xsmjkTh0N6Hds1wsolPpAt+4BqCufiYANnzfV2weNbe
6pW1q7tGaqv3a0tmTZ849szIbxsQDqAZcXNIbHR3zMj4=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *SUBCA QC IZENPE - TSA*

Issuer 2.5.4.97:	*VATES-A01337260*
Issuer O:	*IZENPE S.A.*
Issuer C:	*ES*
Subject CN:	*tsa.izenpe.com*
Subject 2.5.4.97:	*VATES-A01337260*
Subject O:	*IZENPE S.A.*
Subject C:	*ES*
Valid from:	*Fri Oct 30 14:54:16 CET 2020*
Valid to:	*Thu Oct 30 14:54:16 CET 2025*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C8:3B:18:B4:5D:2C:83:AD:52:90:38:38:1B:B9:23:CB:49:60:1F:D5:B7:13:92:E5:8B:3A:AE:4E:9E:86:6F:9C:6E:74:FF:75:D0:03:6C:2D:1A:F7:E3:6A:C4:8F:98:0A:41:46:BC:A5:48:3B:0D:4D:6B:8C:54:E3:22:D5:2A:46:F3:60:6A:44:3A:F9:6D:3B:CE:FE:77:1F:DF:59:C3:87:E7:E6:1C:E2:25:97:70:21:DE:69:C8:66:AD:70:2A:0E:FF:B5:C2:B6:06:55:00:5C:E7:03:DC:08:F0:14:63:7A:95:D3:DC:02:20:5C:77:AB:14:85:0B:05:BD:79:2A:12:68:01:4F:8C:1F:09:C4:B6:16:69:DE:68:B9:CD:5A:F1:69:86:14:F6:3E:87:87:DB:92:57:99:17:1E:39:54:45:4B:38:3F:05:25:C7:4C:96:82:05:D5:A5:BB:2C:03:04:AE:FB:41:AF:BD:52:29:E0:23:EF:84:4D:D6:EF:7C:9C:7D:E5:74:36:28:A1:3A:AB:91:B0:9B:B1:02:F6:43:69:E2:3B:71:7E:52:99:86:79:96:1E:2B:05:7D:AB:E4:7F:B9:A8:D8:18:04:AE:F7:E9:C2:08:F5:D8:DE:79:22:52:FC:36:F8:BE:48:9F:6C:86:A6:03:17:D4:16:B7:F5:3A:DE:76:40:33:B7:08:51:CD:24:30:1C:5A:13:82:46:70:D5:E4:AF:13:BE:0C:E1:DA:54:0D:2F:F3:AE:27:7B:B1:52:8A:72:36:1C:39:08:AB:15:18:3F:FC:D6:90:3A:44:07:CF:9D:8C:CA:82:37:5D:D6:12:25:B7:5F:7D:D4:20:06:48:95:94:03:82:4C:DE:ED:97:2C:05:D6:D2:AD:91:DE:78:0C:58:B8:92:CE:51:B3:11:77:17:88:02:C1:AC:56:F8:ED:F6:20:E0:65:05:E3:C3:6A:6B:FB:4A:B7:E9:F1:B3:D7:B2:23:7C:32:1D:2D:41:10:B0:7C:52:C0:70:02:C5:51:A4:F9:8A:93:3E:8A:B2:29:D5:38:E0:06:7F:8E:A5:C8:3B:9B:96:0D:26:58:F1:0E:74:DA:50:C3:E6:19:C7:A4:7A:E7:6E:32:81:C8:D9:48:86:A7:82:6C:D1:21:C5:AD:35:3E:E6:33:FC:DE:7D:92:AB:09:9C:4E:EB:B5:E4:B4:0A:3E:AE:9D:FB:9E:53:99:4A:C8:19:40:AF:BC:D5:CB:2B:46:1E:8F:77:6E:E1:7A:A0:B2:5C:7C:95:3B:7B:46:6F:3E:77:00:20:6E:55:E0:82:03:E1:6A:08:64:C2:A0:D4:82:C5:50:F4:3F:78:F5:BA:3F:91:90:3B:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*6E:72:03:7C:9F:66:79:AD:E9:6B:5A:3B:B8:71:3F:8D:6F:BC:ED:CC*
Authority Key Identifier	*EA:84:45:BA:7F:5C:49:FB:15:0B:A3:0F:0E:8D:9C:E4:3F:AB:A2:C1*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.14777.10.1* *CPS pointer: http://www.izenpe.eus/cps* *CPS text: [Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado]*
Authority Info Access	*http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SUBCA_QC_TSA.crt*
CRL Distribution Points	*http://crl.izenpe.eus/cgi-bin/izenpeTSA*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D0:96:8A:07:3A:C6:46:F6:86:AC:CD:A8:44:BB:A6:CE:83:0C:D0:E1:A2:F4:E2:28:DB:A6:73:47:C9:F3:61:7C*

X509SubjectName

Subject CN:	*tsa.izenpe.com*
Subject 2.5.4.97:	*VATES-A01337260*

Subject O:	*IZENPE S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*bnIDfJ9mea3pa1o7uHE/jW+87cw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-04-21T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

17 - TSP: Firmaprofesional, S.A.

.

TSP Name

Name	[en]	*Firmaprofesional, S.A.*
Name	[es]	*Firmaprofesional, S.A.*

TSP Trade Name

Name	[en]	*Firmaprofesional, S.A.*
Name	[es]	*Firmaprofesional, S.A.*
Name	[en]	*VATES-A62634068*
Name	[en]	*Firmaprofesional S.A. NIF A-62634068*
Name	[en]	*Firmaprofesional SA*
Name	[en]	*Firmaprofesional S.A.*

PostalAddress

Street Address	[en]	*Paseo de la Bonanova, 47*
Locality	[en]	*Barcelona*
State Or Province	[en]	*Barcelona*
Postal Code	[en]	*8017*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*Paseo de la Bonanova, 47*
Locality	[es]	*Barcelona*
State Or Province	[es]	*Barcelona*
Postal Code	[es]	*8017*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:info@firmaprofesional.com*

URI	*[en]*	*http://www.firmaprofesional.com*

TSP Information URI

URI	*[en]*	*http://www.firmaprofesional.com*
URI	*[es]*	*http://www.firmaprofesional.com*

17.1 - Service (withdrawn): Qualified Certificates issued by "AC Firmaprofesional - CA1"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by "AC Firmaprofesional - CA1"*
Name	*[es]*	*Certificados reconocidos emitidos por "AC Firmaprofesional - CA1"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5994315158441080934*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIF3DCCA8SgAwIBAgIIUzAV4JqeuGYwDQYJKoZIhvcNAQEFBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwgQ0lGIEE2
MjYzNDA2ODAcFw0wOTA4MjUxMDA1NTRaFw0zMDA2MTYxMDA1NTRaMIIBFjELMAkGA1UEBhMCRVMx
JzAlBgkqhkiG9w0BCQEWGGNhMUIBmaXJtYXByb2Zlc2lvbmFsLmNvbTEsMCAGA1UEBxMZQy8gTXVu
dGFuZXIgNfQ0IEJhcmNlbG9yYTExMCNGA1UECxMoQ29uc3VsdGUgaHR0cDovL3d3dy5maXJtYXBy
b2Zlc2lvbmFsLmNvbTE0MDIGA1UECxMrSmVyYXJxdWlhIGRlIENlcnRpZmlj YWNpb24gRmlybWFw
cm9mZXNpb25hbDEtMCsGA1UEChMkRmlybWFwcm9mZXNpb25hbCBTLkEuIE5JRiBBLTYyNjM0MDY4
MSIwIAYDVQQDExlBOyBGaXJtYXByb2Zlc2lvbmFsIC0gQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAx6ueMINjb6t6dcq8ak6BWbjIZ2jEFapQyGdYLolQAY94yiPaX/i3XEJEga
nwqIfG63okc/PWRU/e8Q6QhJVTNR4yOaVxbGFvF9nlk9T7425YChgqoru0T/o8iU6ltZJ8byZSH
iuZnycOwEFVZ6eQX9CyvJ/vNhCMW1iXTuQKLckU3CSSAPHKYEE0m1FMhbArWazbI0eFk8/9VHFf9
/ZyyyaThZEyE+OFs2i8r7fADsd7wzeFxSjqyVouFOnOtu0YUV6vpl4hCcNqsN4A5TupRCfIPx9I5
r4dC8zuCILNBq6JEPzjb73sFU3HFvxXTcVpVbXUxpLQzC0f6xNZD0bUwIDAQABo4HwMIHtMBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUZc3rqzI/eAD5+1XTAHLRzRw4aZC8wOwYDVR0fBDQw
MjAwoC6gLIYqaHR0cDovL2NybC5maXJtYXByb2Zlc2lvbmFsLmNvbS9mcHJvb3QuY3JsMA4GA1Ud
DwEB/wQEAwIBBjAdBgNVHQ4EFgQUi1BXWsG9kgCmt+WFXcPdtrWGkNIwSgYDVR0gBEMwQTA/Bgor
BgEEAYpbCgoBMDEwLwYIKwYBBQUHAgEWI2h0dHA6L y93d5cuZmlybWFwcm9mZXNpb25hbCSjb20v
Y3BzMA0GCSqGSIb3DQEBBQUAA4ICAQBVflkYOaplyB9sBjEEfyUzpFFUdl3xVJTBPLLBPz9t/OwI
K7Xzfanm/QLQT1D5gcOUpPaSUFrh98al+RUSLDHCwKwzniwjQpZs2ggp+n8XNSVcX+oSS+okj4ov
OT7JbY0IY9X Vt3rhf0CvpppzEqqPaSqbo6Cq08vZ+JgGRXmekdvT3L44NUOtgfjnF9lUoXoZXiCM
PjM0tHzZTFBv0lbuXjhn61dZ0OUHZJN9LRCktr0FuRzOjVIbvlmuq+zlqXZqsLXM8i3ONvq+nlm
DC/a2sqkCi2oyAa4OvRAaS4YO6c1PPe2A+JHDuIRjT1u7IDZBQqS1vWsu4r1SnOsjkCtmRzw3lSZ
XCcP27JpNqyJVti6JwQ0DFetMtalhXDeqRvuTyIdHes3VWDpBw6SRTccmI6Yz2ZiL2k27fjo4Ewo
yihMkSXtFkBiTQWym0FoWBZFb436GQlygn5BczHlTHRlvKZ0fx4NcIzr2pYVFqnTSzKFA6a6R30s
v7Q2U/05GlIsYOpnoraKSahZOIKP0uIGr+e/iF0j7kyVDlUSvwnSNXY/LM3slsR+e2s+kacIXXO/s
zONkuszrT5h67sRt/SuT4SfpWb6pMD90LmvtXIlJcXEzTMM4b/TyKqPBkzgJd5HPgsVITJI33u
4LYOvS0rb/RBIGXsRG3pC4ihftt6OQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - CA1*

Subject O: *Firmaprofesional S.A. NIF A-62634068*

Subject OU: *Jerarquia de Certificacion Firmaprofesional*

Subject OU: *Consulte http://www.firmaprofesional.com*

Subject L: *C/ Muntaner 244 Barcelona*

Subject E: *ca1@firmaprofesional.com*

Subject C: *ES*

Valid from: *Tue Aug 25 12:05:54 CEST 2009*

Valid to: *Sun Jun 16 12:05:54 CEST 2030*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:AB:9E:30:93:63:6F:A8:BA:B5:DC:6A:F1:A9:3A:05:66:E3:95:9D:B7:8C:41:5A:A5:0C:86:75:82:E8:95:00:18:F7:8C:A2:3D:A5:FF:8B:75:C4:24:4A:9A:9F:0A:A5:7C:6E:B7:A2:47:3F:3D:64:65:FE:57:BC:43:A4:21:25:54:CD:47:8C:8E:69:5C:5B:18:5B:C5:F6:72:24:F5:3E:F8:DB:96:02:86:0A:A8:AE:ED:13:FE:8F:22:53:A2:2D:64:9F:1B:C9:94:87:8A:E6:67:C9:C3:B0:10:55:59:E9:E4:17:F4:2C:AF:27:FB:CD:84:23:16:D6:25:D3:B9:02:8B:72:45:37:09:24:80:3C:72:98:10:4D:26:D4:53:21:6C:0A:D6:6B:36:C8:D1:E1:64:F3:FF:55:1C:57:FD:FD:9C:B2:C9:A4:E1:64:4C:84:F8:E1:6C:DA:2F:2B:ED:F0:03:B1:DE:F0:CD:E1:71:4A:36:A3:56:8B:85:3A:73:AD:BB:46:14:57:AB:E9:97:88:42:70:DA:AC:37:80:39:4E:EA:51:09:FB:4F:C7:D9:79:AF:87:4E:82:E0:89:2C:D0:6A:E8:91:0F:7A:36:FB:DE:C1:54:DC:71:6F:89:74:DC:56:95:61:5D:4C:69:2D:0C:CE:7F:AC:4D:64:3D:1B:53:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Subject Key Identifier *8B:50:57:5A:C1:BD:92:00:A6:B7:E5:85:5D:C3:DD:B6:B5:86:90:D2*

Certificate Policies *Policy OID: 1.3.6.1.4.1.1377.10.10.1*

CPS pointer: http://www.firmaprofesional.com/cps

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0E:BB:DF:14:6E:63:F7:0F:AA:59:27:EE:8E:53:46:E9:C9:6C:5F:0D:9B:DD:32:12:B0:4E:D6:68:71:79:87:4D*

Certificate fields details

Version: *3*

Serial Number: *124*

X509 Certificate

-----BEGIN CERTIFICATE-----

*MIIGiTCCBXGgAwIBAgIBfDANBgkqhkiG9w0BAQUFADCBnTELMAkGA1UEBhMCRVMxIjAgBgNVBAcT
GUMvIE11bnRhbmVyIDI0NCBCYXJfZWxvbmExQjBABgNVBAMTOUFIdG9yaWRhZCBkZSBDZXJ0aWZp
Y2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwgQ0lGIE2MjYzNDA2ODEmMCOGCSqGSIb3DQEJARYXYY2FA
ZmlybWFwcm9mZXNpb25SbC5jb20wHhcNMDMwMzI3MTE1MTM4WhcNMTMwMzI1MjMwMDAwWjCCARYx
CzAJBgNVBAYTAkVTMScwJQYJKoZIhvcNAQkBFhhjYTFAZmlybWFwcm9mZXNpb25SbC5jb20xIjAg
BgNVBAcTGUMvIE11bnRhbmVyIDI0NCBCYXJfZWxvbmExMTAvBgNVBAsTKENvbnN1bHRlIGh0dHA6
Ly93d3cuZmlybWFwcm9mZXNpb25SbC5jb20xNDAyBgNVBAsTK0pfcmFycXVpYSBkZSBDZXJ0aWZp
Y2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwxLTArBgNVBAoTJEZpcm1hcHJvZmVzaW9uYWwgUy5BLiBO
SUYgQS02MjYzNDA2ODEiMCAGA1UEAxMZQUMgRmlybWFwcm9mZXNpb25SbCAtIENBMTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMernjCTY2+ourXcavGpOgVm45Wdt4xBWqUMhnWC6JUA
GPeMoj2l/4t1xCRKmp8KpXxut6JHPz1kZI5XvEOkISVUzUeMjmlcWxhbxIZyJPU++NuWAoYKqK7t
E/6PlI0iLWStG8mUb4rmZ8nDsBBVWenkF/Qsry7ZyQjFrYI07kC/3JFNwkkgDxymBBNJtRTIWwK
1ms2yNHhZPPVRxX/f2cssmk4WRMbPjhbNonK+3wA7Hc8M3bcUo2o1aLbTpzrbGFFerr6zeIQnDa
rDcAOU7qUQn7T8Zea+HToLgiSzQauiRD3o2+97BVNxxb4l03FaVYV1MaS0Mzn+sTWQ9G1MCAwEA
AaOCAIYwggJSMCoGA1UdEgQjMCGGH2h0dHA6Ly93d3cuZmlybWFwcm9mZXNpb25SbC5jb20wKgYD
VR0RBCMwIYYfaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbTASBgNVHRMBAf8ECDAGAQH/
AgEAMA4GA1UdDwEB/wQEAwIBBjARBglghkgBhvhCAQEEBAMCAAcwQgYJYIZIAYb4QgEIBC0WK2h0
dHA6Ly93d3cuZmlybWFwcm9mZXNpb25SbC5jb20vY3BzL2Nwcy5odG0wHQYDVR0OBBYEFltQV1rB
vZIAprflhV3D3ba1hpDSMlHKBgNVHSMEgcIwgb+AFDMLoGbR6trO3mKTBChStRR/OGi3oYGjpIGg
MIGdMQswCQYDVQQGEwJFUzEiMCAGA1UEBxMZQy8gTXVudGFuZXIgMjQ0IEJhcmNlbG9uYTFCMEAG
A1UEAxM5QXV0b3JpZGRlKGRlIENlcnRpZmlyYWNpb24gRmlybWFwcm9mZXNpb25SbCBDSUYgQTYy
NjM0MDY4MSYwJAYJKoZIhvcNAQkBFhdjYUBmaXhYXByb2Zlc2lvbmFsLmNvbYIBATBSBgNVHSAE
SzBJMEcGCisGAQQB5nkKCgEwOTA3BggrBgEFBQcCARYraHR0cDovL3d3dy5maXhYXByb2Zlc2lv
bmFsLmNvbS9jcHMvY3BzLmh0bTBFBgNVHR8EPjA8MDagOKA2hjRodHRwOi8vY3JsLmZpcm1hcHJv
ZmVzaW9uYWwuY29tLZpcm1hcHJvZmVzaW9uYWwuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQBC7y1f
qWCESvfTo1yoobu6S3jcOA6R/35WcIU9Wt0mGZ+A6drP5T2+IvY7w9x1LKztKr6QIh9KasJkZm1
sIzAHD7HEW/OMyVI4Fos1hj8ZNWjqeWo1SRUlEDQ0VmZrsoyTPAMoq9uy0Xbg4Tu83T3nM1qpol
Adej2Gv3xPltcSnmDPskQy3BSGACWVSMBD82uWxNccvUMIFh1pZwwHiSq6UqSkst+qPnjQLsOn6L
pAajPT7iLi3pQny9ZXzYd+oY2e/qWZLWsgyygjQ9RmB6D9KgP38FqvkO40+mg88jIJfnONAEni
dZqE2dmcs8LdV0OFz+Gi1U7z1oaLiN8*

-----END CERTIFICATE-----

Signature algorithm:	*SHA1withRSA*
Issuer E:	*ca@firmaprofesional.com*
Issuer CN:	*Autoridad de Certificacion Firmaprofesional CIF A62634068*
Issuer L:	*C/ Muntaner 244 Barcelona*
Issuer C:	*ES*
Subject CN:	*AC Firmaprofesional - CA1*
Subject O:	*Firmaprofesional S.A. NIF A-62634068*
Subject OU:	*Jerarquia de Certificacion Firmaprofesional*
Subject OU:	*Consulte http://www.firmaprofesional.com*
Subject L:	*C/ Muntaner 244 Barcelona*
Subject E:	*ca1@firmaprofesional.com*
Subject C:	*ES*
Valid from:	*Thu Mar 27 12:51:38 CET 2003*
Valid to:	*Tue Mar 26 00:00:00 CET 2013*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:AB:9E:30:93:63:6F:A8:BA:B5:DC:6A:F1:A9:3A:05:66:E3:95:9D:B7:8C:41:5A:A5:0C:86:75:82:E8:95:00:18:F7:8C:A2:3D:A5:FF:8B:75:C4:24:4A:9A:9F:0A:A5:7C:6E:B7:A2:47:3F:3D:64:65:FE:57:BC:43:A4:21:25:54:CD:47:8C:8E:69:5C:5B:18:5B:C5:F6:72:24:F5:3E:F8:DB:96:02:86:0A:A8:AE:ED:13:FE:8F:22:53:A2:2D:64:9F:1B:C9:94:87:8A:E6:67:C9:C3:B0:10:55:59:E9:E4:17:F4:2C:AF:27:FB:CD:84:23:16:D6:25:D3:B9:02:8B:72:45:37:09:24:80:3C:72:98:10:4D:26:D4:53:21:6C:0A:D6:6B:36:C8:D1:E1:64:F3:FF:55:1C:57:FD:FD:9C:B2:C9:A4:E1:64:4C:84:F8:E1:6C:DA:2F:2B:ED:F0:03:B1:DE:F0:CD:E1:71:4A:36:A3:56:8B:85:3A:73:AD:BB:46:14:57:AB:E9:97:88:42:70:DA:AC:37:80:39:4E:EA:51:09:FB:4F:C7:D9:79:AF:87:4E:82:E0:89:2C:D0:6A:E8:91:0F:7A:36:FB:DE:C1:54:DC:71:6F:89:74:DC:56:95:61:5D:4C:69:2D:0C:CE:7F:AC:4D:64:3D:1B:53:02:03:01:00:01*
Issuer Alternative Name	*http://www.firmaprofesional.com*
Subject Alternative Name	*http://www.firmaprofesional.com*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*8B:50:57:5A:C1:BD:92:00:A6:B7:E5:85:5D:C3:DD:B6:B5:86:90:D2*
Authority Key Identifier	*33:0B:A0:66:D1:EA:DA:CE:DE:62:93:04:28:52:B5:14:7F:38:68:B7*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.13177.10.10.1* *CPS pointer: http://www.firmaprofesional.com/cps/cps.htm*
CRL Distribution Points	*http://crl.firmaprofesional.com/firmaprofesional.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *65:BA:8F:C0:CE:3C:43:41:64:DC:40:81:5A:6C:A6:FB:44:C7:27:20:46:FC:D3:03:A2:9D:A8:F4:1C:A2:07:5D*

X509SubjectName

Subject CN: *AC Firmaprofesional - CA1*

Subject O: *Firmaprofesional S.A. NIF A-62634068*

Subject OU: *Jerarquia de Certificacion Firmaprofesional*

Subject OU: *Consulte http://www.firmaprofesional.com*

Subject L: *C/ Muntaner 244 Barcelona*

Subject E: *ca1@firmaprofesional.com*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-11-16T00:00:00Z

17.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.2*

17.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by "AC Firmaprofesional - CA1"*

Name *[es]* *Certificados reconocidos emitidos por "AC Firmaprofesional - CA1"*

Service digital identities

X509SubjectName

Subject CN: *AC Firmaprofesional - CA1*

Subject O: *Firmaprofesional S.A. NIF A-62634068*

Subject OU: *Jerarquia de Certificacion Firmaprofesional*

Subject OU: *Consulte http://www.firmaprofesional.com*

Subject L: *C/ Muntaner 244 Barcelona*

Subject E: *ca1@firmaprofesional.com*

Subject C: *ES*

X509SKI

X509 SK I *i1BXWsG9kgCmt+WFXcPdtrWGkNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

17.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.2*

17.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by "AC Firmaprofesional - CA1"*
Name	*[es]*	*Certificados reconocidos emitidos por "AC Firmaprofesional - CA1"*

Service digital identities

X509SubjectName

Subject CN:	*AC Firmaprofesional - CA1*
Subject O:	*Firmaprofesional S.A. NIF A-62634068*
Subject OU:	*Jerarquia de Certificacion Firmaprofesional*
Subject OU:	*Consulte http://www.firmaprofesional.com*
Subject L:	*C/ Muntaner 244 Barcelona*
Subject E:	*ca1@firmaprofesional.com*
Subject C:	*ES*

X509SKI

X509 SK I	*i1BXWsG9kgCmt+WFXcPdtrWGkNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

17.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.5.2*

17.2 - Service (granted): Emisión de certificados reconocidos (AAPP)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Emisión de certificados reconocidos (AAPP)*
Name	*[en]*	*Qualified Certificates Issuance (AAPP)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6439481296531745112*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGszCCBJugAwIBAgIIWV2iHxGL6VgwDQYJKoZIhvcNAQEFBQAwUTELMAkGA1UEBhMCRVMxOjBA
BgNVBAMMOUFJdG9yaWRhZCBkZSBDZXI0aWZpY2FjaW9uIEZpcm1hcHIvZmVzaWxuYWwgQ0lGIE2
MjYzNDA2ODAeFw0xMDA3MDcwOTM1NDNaFw0yMjA3MDcwOTM1NDNaMIGkMQswCQYDVQQGEwJFUzEc
MBoGA1UEChMTRmlybWFwcm9mZXNpb25hbCBTQTE+MDwGA1UECxM1Q2VydGlmaWNhZG9zIERpZ2l0
YWxlcyBwYXJhIGxhIEFkbWluaXN0cmFjaW9uIFB1YmxpY2ExEjAQBgNVBAUTCUE2MjYzNDA2ODEj
MCEGA1UEAxMqQUMgRmlybWFwcm9mZXNpb25hbCAtIEFBLUFAwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCrlukO1T1uQPOyCB76CS+Jx8Y3aDlvsVVVwPcuIQGopfn3dEtE3+q5g3dJT1Cp
+6RIQI3Of38kXLzCB26SLj4up1L3CmVZ75Kqeg/GqmOtlgM1sZnAGIQiXpoVt+AloQo1XhqRhen4
UDqH+8k0X8pHZc4BXqoKYLiPXrpnC68bjKlZCYy1FKbGUEXULKzt4rb9XzZaw27AJFunV9SKpRUc
AZQDDORvEZqnVq7wcTwdkNloRL1R/NpjXrQQdGoA8mFoVMpKMyI5P8tuaYcE1AKpdTznNC7sPDHW
BMoO7U4Z18PD8Un/QNj4pXbWpTV79fBnZkLS1uREC1QUZL2E+mkFAgMBAAGjggI5MIICNTBGBggr
BgEFBQcBAQQ6MDgwNgYIKwYBBQUHMAGGKmh0dHA6Ly9zZXJ2aWNpb3MuZmlybWFwcm9mZXNpb25h
bC5jb20vb2NzcDAdBgNVHQ4EFgQUpi7qTSUrIbqkidog0h2u55b9mfcwEgYDVR0TAQH/BAgwBgEB
/wIBADAfBgNVHSMEGDAWgBRbcurNR4APn7VdMActHNHDhpkLzCCAUcGA1UdIASCATwggE6MIIB
NgYKKwYBBAHmeQoKATCCASYwLwYIKwYBBQUHAgEWI2h0dHA6Ly9sZCuZmlybWFwcm9mZXNpb25h
bC5jb20vY3BzMIHyBggrBgEFBQcCAjCB5R6B4gBDAGUAcgB0AGkAZgBpAGMAYQBkAG8AIABkAGUA
IABBAHUAdABvAHIAaQBkAGEAZAAgAGQAZQAgAEMAZQByAHQAaQBmAGkAYwBhAGMAaQDzAG4ALgAg
AEMAbwBuAHMAdQBsAHQAZQAgAGwAYQBzACAAYwBvAG4AZABpAGMAaQBvAGAAZQBzACAAZABlACAA
dQBzAG8AIABlAG4AIABoAHQAdABwADoALwAvAHcAdwB3AC4AZgBpAHIAbQBhAHAAegBvAGYAZQBz
AGkAbwBuAGEAbAAuAGMAbwBtAC8AYwBwAHMwPAYDVR0fBDUwMzAxoC+gLYYraHR0cHM6Ly9jcmwu
ZmlybWFwcm9mZXNpb25hbC5jb20vZnByb290LmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcN
AQEFBQADggIBAHI5+CAhX88GSnBHO4nxQ+fZTWNiHU9tU269LSuERZXO301Gob6ooI5KYCGSK/C
sFB2Ya6gJvfq5zbWxaSAtDbxE0+QGfg11TKID1BSaFBtuScFTu/3jbmUlRyrR+67S6HZk+t4VxEV
vHgO/BH3lq/rWdgAg57zRsYLWx+JD/+UfWh+D+pljOS53CbKud00I6nGTF5yD/SklONXp1AIBt2W
Z2KxpOEsVzxs4HNB1ZHJhBhCSHCPJFtgw/2+C28Ylz6BX49bSTvJSGfo5hNPwrozR6m8+Lz4Ndtb
/jG9K3fNwe+0zZPZTwzkrUJ7RZYHOMT+XHJAPLdW8zk0s+l2uXy/t0KAS3TcT9KIM1J0XRUqsHp
kqJG7b6W/To8dXhzukI0mZm2wzEWMGKHDzNt7dUSNXycSmraAhXKIqQQCJkYFbYYTnIV0vyy2zZU
p39AgzB6Zv/KuMnG3IPn0JHz+plAqz0hlMuU77Covspsk/DpyztNafsyDFbuq1nzCZP82ppc/6ul
7WXZ6oaBNDBeTuhLvyqt9srnJ4IbhupERp6JEGDYUdmS9xY44gfQr7AAot0pwrWNc5PLScUMGHNd
AdsXNl7nbRH+jP2QwqUPmFNAkosbb1OTHOzICMPBpUUuqWctkSojlQ35o0UVqKM7rfDcE0mlkQ
egiIjKYg+50k
-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C:	*ES*
Subject CN:	*AC Firmaprofesional - AAPP*
Subject SERIAL NUMBER:	*A62634068*
Subject OU:	*Certificados Digitales para la Administracion Publica*
Subject O:	*Firmaprofesional SA*
Subject C:	*ES*
Valid from:	*Wed Jul 07 11:35:43 CEST 2010*
Valid to:	*Thu Jul 07 11:35:43 CEST 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AB:96:E9:0E:D5:3D:6E:40:F3:B2:08:1E:FA:09:2F:89:C7:C6:37:68:39:6F:B1:55:55:C0:F7:2E:21:01:A8:A5:F9:F7:74:4B:44:DF:EA:B9:83:77:49:4F:50:A9:FB:A4:5F:40:8D:CE:7E:7F:24:5C:BC:C2:07:6E:B9:2E:3E:2E:A7:52:F7:0A:65:59:EF:92:AA:7A:0F:C6:AA:63:AD:96:03:35:B1:99:C0:18:84:22:5E:9A:15:B7:E0:25:A1:0A:35:5E:1A:91:85:E9:FB:50:3A:87:FB:C9:34:5F:CA:47:65:CE:01:5E:AA:0A:60:B8:8F:5E:B8:E7:0B:AF:1B:8C:AD:59:09:8C:B5:14:A6:C6:50:45:D4:2C:AC:ED:E2:B6:FD:5F:36:5A:C3:6E:C0:24:5B:A7:57:D4:8A:A5:15:1E:03:64:03:0D:04:6F:11:9A:A7:56:AE:F0:71:3C:25:90:D2:28:44:B9:51:FC:DA:63:5F:14:10:74:6A:00:F2:61:68:54:CA:4A:33:22:39:3F:C4:67:69:87:04:24:02:A9:75:3C:E7:34:27:F1:3C:31:D6:04:CA:0E:ED:4E:19:D7:C3:C3:F1:49:FF:40:D8:F8:A5:78:56:A5:35:7B:F5:F0:67:66:42:D2:D6:E4:44:08:84:14:64:BD:84:FA:69:05:02:03:01:00:01*
Authority Info Access	*http://servicios.firmaprofesional.com/ocsp*
Subject Key Identifier	*A6:2E:EA:4D:25:2B:25:BA:A4:B5:DA:20:D2:1D:AE:E7:96:FD:99:F7*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.13177.10.10.1* *CPS pointer: http://www.firmaprofesional.com/cps* *CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]*
CRL Distribution Points	*https://crl.firmaprofesional.com/fproot.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*83:F6:F0:17:C2:53:6D:74:54:B7:B9:84:86:74:F3:64:01:29:CF:55:5D:D0:7D:83:D3:62:A1:7C:81:B7:52:5F*

Certificate fields details

Version:	*3*
Serial Number:	*7893570382112079418*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIG2jCCBMKgAwIBAgIIbYuYcMtVvjowDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUFJdC9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIFZpcm1hcHJv2mVzaWNuYWwgQ0lGIEi2
MjYzNDA2ODAeFw0xNjEwMjUxNTA4MDNaFw0yMjA3MDkwODM1NDNaMGkMQswCQYDVQQGEwJFUzEc
MBoGA1UECgwTRmlybWFwcm9mZXNpb25hbCBTQTE+MDwGA1UECwwI Q2VydGlmaWNhZG9zIERpZ2l0
YWxlcyBwYXJhIGxhIEFkbWluaXN0cmFjaW9uIFB1YmxpY2ExEjAQBgNVBAUTCUE2MjYzNDA2ODEj
MCEGA1UEAwwaQUMgRmlybWFwcm9mZXNpb25hbCAtIEFBUFAwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCrlak01TxQPOyCB76CS+Jx8Y3aDlvsVVVwPxufQGopfn3dEtE3+q5g3dTTCp
+6RfQI3OI38kXLzCB265Lj4up1L3CmVZ75Kqeg/GqmOtlgM1sZnAGIQiXpoVt+AloQo1Xhqkhen4
UDqH+8k0X8pHZc4BXqoKYLiPXrjnC68bjK1ZCYy1FKbGUEXULKzt4rb9XzZaw27AJFunV9SKpRUc
A2QDDQRvEZqnVq7wcIwlkNloRLlR/NpjXxQQdGoA8mFoVMpKMy15P88naYcEJAKpdTznNCfxPDHW
BMoO7U4Z18PD8Uln/QNj4pXbWpTV79fBnZkLS1uREcIQUZL2E+mkFAgMBAAGjggIgMIICXDB0Bggr
BgEFBQcBAQRoMGYwNgYIKwYBBQUHMAKGKmh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20v
Y2Fyb290LmNydDAsBggrBgEFBQcwAYYgaHR0cDovL29jc3AuZmlybWFwcm9mZXNpb25hbC5jb20w
HQYDVR0OBBYEFKYu6k0lKyW6pLXaINldrueW/Zn3MBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0j
BBgwFoAUZcSrqzUcAD5+1XTAHLRzRw4aZC6wggFBBgNVHSAEggE4MIIBNDCCATAGBFUdIAAwggEm
MIHyBggrBgEFBQcCAjCB5R6B4gBDAGUAcgB0AGkAZgBpAGMAYQBkAG8AIABkAGUAIABBAHUAdABv
AHIAaQBkAGEAZAAgAGQAZQAgAEMAZQByAHQAaQBmAGkAYwBhAGMAaQDzAG4ALgAgAEMABwBuAHMA
dQBsAHQAZQAgAGwAYQBzACAAYwBvAG4AZABpAGMAaQBvAGAAZQBzACAAZABlACAAdQBzAG8AIABl
AG4AHBoAHQAdABwAIoALwAvAHcAdwB3AC4AZgBpAHIAbQBhAHAAcgBvAGYAZQBzAGkAbwBuAGEA
bAAuAGMAbwBtAC8AYwBwAHMwLwYIKwYBBQUHAgEWI2h0dHA6Ly93dEcuZmlybWFwcm9mZXNpb25h
bC5jb20vY3BzMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5j
b20vZnByb290LmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBADFNkXHvZUBr
Zspcmv9HinSbbVjNkUVNT+70h55BNycD0cO6laGdjzagguNab50G0C8ULnj7Wcktbsrl4pjYAwqw1
FYFTLbxPKlczZHP9S0UeSc6sEUZPW/b4qoaA9Iv5PO4xGXDA6Rk9fqZGdKsAyz86faSV4o9RL1NS
GZajTt9e1t5yWQjThSoyv+xxi9D80u3f+5B+ZcrPT6tNdP08EtB1npXpI5NsD52nj2NimH/C5lUD
CS35zRdjrNAzvcYBncCYB3aZqcNRk+VNgFpbQv1xyQJqkvMikex6HyIawzxLvoEAbUW8nl0s2ts+
PqYUWiYSvK9YsHnEdlvqHv1RbTWh6kPXjPsAeJ6fnkLYzUvnqLTNT3xdIxuJ4Rarq6E0LIJqpn
hxg+IDL5GXV3KB7icpgbsBCEwS+TFIXcxvYxFkkK3axiRz9+WjclmXuUOh3m1IeLFur26FZsqb5
RaJ96HgATl3bEb2gkuGVg6OoLwbkEvXUPDtObjG+T3oU+4pGe5fiwTEW+NrQiM3jC1d1Xcc0eYre
ph7k72wCg09A0rPTbFRBQ+H8wCjRH+rcB0YXv4ejZNFNv4iHrEzGPTmPO988h8o8UiNMLvFacY+2
uWnpyhmpQw9meV/gTia72qFXtOTNBvB6rgYBZ05XPkvARkYhGDBMmCKOIsDNHJ/t

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - AAPP*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Digitales para la Administracion Publica*

Subject O: *Firmaprofesional SA*

Subject C: *ES*

Valid from: *Tue Oct 25 17:08:03 CEST 2016*

Valid to: *Thu Jul 07 10:35:43 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AB:96:E9:0E:D5:3D:6E:40:F3:B2:08:1E:FA:09:2F:89:C7:C6:37:68:39:6F:B1:55:55:C0:F7:2E:21:01:A8:A5:F9:F7:74
:4B:44:DF:EA:B9:83:77:49:4F:50:A9:FB:A4:5F:40:8D:CE:7F:7F:24:5C:BC:C2:07:6E:B9:2E:3E:2E:A7:52:F7:0A:65:59:EF:92:AA:7A:0F:C6:AA:63:AD:96:03:35:B1:99:C0:18:84:22:5E:9A:15:B7:E0:25:A1:0A:35:5E:1A:91:
85:E9:F8:50:3A:87:FB:C9:34:5F:CA:47:65:CE:01:5E:AA:0A:60:B8:8F:5E:B8:E7:0B:AF:1B:8C:AD:59:09:8C:B5:14:A6:C6:50:45:D4:2C:AC:ED:E2:B6:FD:5F:36:5A:C3:6E:C0:24:5B:A7:57:D4:8A:A5:15:1E:03:64:03:0D:0
4:6F:11:9A:A7:56:AE:F0:71:3C:25:90:D2:28:44:B9:51:FC:DA:63:5F:14:10:74:6A:00:F2:61:68:54:CA:4A:33:22:39:3F:C4:67:69:87:04:24:02:A9:75:3C:E7:34:27:F1:3C:31:D6:04:CA:0E:ED:4E:19:D7:C3:C3:F1:49:FF:40:D8
:F8:A5:78:56:A5:35:7B:F5:F0:67:66:42:D2:D6:E4:44:08:84:14:64:BD:84:FA:69:05:02:03:01:00:01

Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier *A6:2E:EA:4D:25:2B:25:BA:A4:B5:DA:20:D2:1D:AE:E7:96:FD:99:F7*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *63:65:B2:5E:92:99:B5:F3:82:EB:00:66:85:06:29:08:8E:BC:D9:BC:B3:98:F2:86:22:10:76:03:C3:C1:C2:7E*

X509SubjectName

Subject CN: *AC Firmaprofesional - AAPP*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Digitales para la Administracion Publica*

Subject O: *Firmaprofesional SA*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-11-16T00:00:00Z

Scheme Service Definition URI

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

17.2.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

17.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

17.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

17.2.4 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Emisión de certificados reconocidos (AAPP)

Name [en] Qualified Certificates Issuance (AAPP)

Service digital identities

X509SubjectName

Subject CN: AC Firmaprofesional - AAPP

Subject SERIAL NUMBER: A62634068

Subject OU: Certificados Digitales para la Administracion Publica

Subject O: Firmaprofesional SA

Subject C: ES

X509SKI

X509 SK I pi7qTSUrJbqktdog0h2u55b9mfc=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

17.2.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.2

17.2.4.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.22.3

17.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

17.2.5 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Emisión de certificados reconocidos (AAPP)

Name [en] Qualified Certificates Issuance (AAPP)

Service digital identities

X509SubjectName

Subject CN: AC Firmaprofesional - AAPP

Subject SERIAL NUMBER: A62634068

Subject OU: Certificados Digitales para la Administracion Publica

Subject O: *Firmaprofesional SA*

Subject C: *ES*

X509SKI

X509 SK I *pi7qTSUrJbqktdog0h2u55b9mfc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-04-28T00:00:00Z*

17.2.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

17.3 - Service (granted): Qualified certificates issued by “AC Firmaprofesional – CUALIFICADOS”

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by “AC Firmaprofesional – CUALIFICADOS”*

Name *[es]* *Certificados reconocidos emitidos por la “AC Firmaprofesional - CUALIFICADOS”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *937705595546249684*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGyDCCBLCgAwIBAgIIDQNmRV5uKdQwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMTOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwgQ0lGIEE2
MjYzNDA2ODAeFw0xNDA5MTgxMDAwNTRaFw0zMDEyMzEwNDAyNTVaMIGSMQswCQYDVQQGEwJFUzEc
MB8wGA1UECMMVR2mhybWFwcm9mZXNpb25lbCBTLkEuMSIwIAYDVQQLExIDZXJ0aWZpY2FkbXMgQ3Vh
bGlmaWNhZG9zMRIwEAYDVQQFEwlBNjI2MzQwNjgxKzApBgNVBAMTIkFDIEZpcm1hcHJvZmVzaW9u
YWwgLSBDVUFMSUZJQ0FET1MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6clIUCaCe
12gMnFsVFePc9Z52zvebPJ30UrhNH0lH4vny6VS7oVOd+aMQvvqW9JmTrYIA1i72jp8TnWNHq0RN
lQMzjid+uQkeVSIOrohSltMejah0hx+vUusoWD5XOdhKV+CCjN+mvcCDUsJWv+jmiN/UVZkHzQRK3M0
cbQRGRNADeKPsrU+B0028OhBgyfOxMr6Sx3BlxXz8r2mXXlFkgtYYOU8zyT4OM+c6mPEmnWL+u
HpuL4MlzvZ/1Rr0+ynyua54bGkb4iijt1a3PecgdY7269FIhlsIWMSnXvKOeY6u6+F+CkkxwqiRO
4xvCEVXY1OblHPpXON3VYWIzLxvIAgMBAAGjggIgMIICXDB0BggrBgEFBQcBAQRoMGYwNgYIKwYB
BQUHMAKGKmhbUlHA6Ly9jcmwuZmlybWFwcm9mZXNpb25lbCSjb20vY2Fvb290LmNydDAsBggrBgEF
BQcwAYYgaHR0cDov1.29jc3AuZmlybWFwcm9mZXNpb25lbCSjb20vaHQYDVR0OBBYEFEtcxzJMHb9HV
hmh9gjpB2UwC+JZdMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUZc3rqzUcAD5+1XTA
HLR2Rw4aZC8wggFBBgNVHSAEggE4MIIBNDCCATAGBFUdIAAwggEmMIHyBggrBgEFBQcCAjCB5R6B
4gBIDAGUAcgB0AGkAZgBpAGMAYQBkAG8AIABkAGUAIABBAHUAdABvAHIAaQBkAGEAZAAgAGQAZQAg
AEMAZQBvAHQAaQBmAGkAYwBhAGMAaQDzAGAAIAgAgAEMAbwBuAHMAdQBsAHQAZQAgAGwAYQBzACAA
YwBvAG4AZABpAGMAaQBvAG4AZQBzACAAZABlACAAdQBzAG8AIABlAG4AIABoAHQAdABwADoALwAv
AHcAdwB3AC4AZgBpAHIAbQBhAHAAcgBvAGYAZQBzAGkAbwBuAGEAbAAuAGMAbwBtAC8AYwBwAHMw
LwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cuZmlybWFwcm9mZXNpb25hbC5jb20vY3BzMDsGA1UdHwQ0
MDIwMKAtoCyGKmhtdHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20vZnByb290LmNybDAOBgNV
HQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAApS6836yufcnOXxNmxxa80WO3iNTO/xiF1s
QH3GfUhNKK9x7QAI2MLTM0FvZ8ZZ23RlLkCnSrYCVI5AJCBvAoE3fxqdV7Q0a45DH7/DNyzTvOEn
yUGHsdWCzCSMXQdi1+fjuLmy+Dr7g9YkqzHNczOVIGg9DOPvXHXUWsSc+06I3hM7YNDsID4hlvo
68NEYPVlo4+qNdk+3edIEA9yRCGoDhNzh1FLQBHZ3WisROVH+9xI6oYhYGNzESGYOIewpxLIbF
6LdyACipm8ywAZg+NRgdDU4ty/+ddP+oBuiRnuzLZZI9zfylC0DQYElcC69LKQ5jc32oAN/k0ns5V
35VKqdEc2JUL0n0zlTDznp1anr/ulTu6sOLChb7LObGZj1BawkMAmZR+2dr1bdVRNJ/hnBhlmspb
/o7wI9rzoBYlMpqGlxHBzpVVJhhO5g1YXqq3X12oSL27xY6LS1/8ifqwtYLovVOzeegr2SgBNDk7M
oIjT1JxoCNG39d+htj1HVceEzp3z+Oc8HlU0Gi98+OnfjO9TzGAz1PjqXa77m3Iu982gsaJH8qK
5DyxGFyMN5CaNg23p/5gATzFrTOF+ipR5+MBaQcDT/zC0tq44ewVc2TcxCN6GbecpMDk67nS1
HSKCZJE/e29hKuGJp3kd1PO1WHlC29XOaKRjmyDC
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - CUALIFICADOS*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Cualificados*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Thu Sep 18 12:00:54 CEST 2014*

Valid to: *Tue Dec 31 05:02:55 CET 2030*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:70:89:54:09:A0:9E:D7:68:0C:9C:5B:15:15:E3:DE:F5:9E:76:CE:F7:9B:3F:F2:77:D1:4A:E1:34:7D:07:E2:F9:F2:E
9:54:BB:A1:53:9D:F9:A3:10:BE:FA:96:F4:99:93:AD:82:00:D6:2E:F6:8E:9F:13:9D:63:47:AB:44:AD:95:03:33:8D:DF:AE:42:47:95:48:83:AB:A2:14:87:31:E8:DA:87:4C:B1:FB:25:2E:B2:85:83:49:73:9D:84:A5:7E:08:28:CD:
FA:7B:DC:08:35:31:25:6F:A3:9A:23:7F:51:56:64:1F:34:11:2B:73:34:71:B4:11:19:13:40:0D:E2:8F:B2:B5:2B:07:4D:36:F0:E8:41:83:23:CE:C4:CE:92:C7:70:48:C5:7C:7C:FC:AF:69:97:5E:D9:45:92:48:2D:55:83:AD:53:CC:F2:4
F:83:8C:F9:CE:A6:3C:49:A7:58:BF:AE:1E:9B:8B:E0:C9:73:BD:9F:F5:46:B3:BE:CA:7C:AE:6B:9E:21:1A:48:78:8A:28:ED:D5:AD:CF:79:C8:1D:63:BD:BA:F4:57:E1:96:C2:16:31:29:D7:BC:A3:9E:63:AB:BA:F8:5F:82:92:
4C:70:AA:24:4E:E3:1B:C2:11:55:D8:D4:E6:C8:1C:F8:17:38:DD:D5:61:62:33:2F:1B:E5:02:03:01:00:01
```


Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points

http://crl.firmaprofesional.com/fproot.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

2B:75:CC:4F:36:75:9C:FC:4C:66:37:B1:E0:E5:43:59:45:7D:B5:7E:74:DE:4D:2D:C5:D0:2C:DD:FF:29:60:CF

Certificate fields details

Version:

3

Serial Number:

9058581230153389879

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGUTCCBDmgAwIBAgIIfbaLomhQVzcwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwgQ0lGIEE2
MjYzNDA2ODAeFw0xODEyMTQxMDEzMjNaFw0zMDEyMzEwNDAyMDBaMIGSMQswCQYDVQQGEwJFUzEe
MBwGA1UEChMVRmlybWFwcm9mZXNpb25lbCBlTLkEuMSIwIAYDVQQLExlDZXJ0aWZpY2FkbzMgQ3Vh
bGlmaWNhZG9zMRIwEAYDVQQFEwlBNjI2MzQwNjgxKzApBgNVBAMTIkFDIEZpcm1hcHJvZmVzaW9u
YWwgLSBDVUFMSUZIQ0FET1MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6cllUCaCe
12gMnFsVFePe9Z52zvebPJ30UrhNH0H4vny6VS7oVOd+aMQvvqW9JmTrYIA1i72jp8TnWNHq0RN
lQMzjd+uQkeVSIOrnbSIMejab0xx+yUssoWDSXOdhKV+CCjN+mvcCDUsJW+jmzN/UVZkHzQRK3M0
cbQRGRNADeKPsrUrB0028OhBgyPOxM6Sx3BlxXz8r2mXXilFkkgtVYOtU8zyT4OM+c6mPEmnWL+u
HpuL4MIzvZ/1RrO+ynyua54bGkb4iijt1a3PecgdY7269FfhlsIWMSnXvKOeY6u6+F+CkkxwqiRO
4xvCEVXY1ObIHPgXON3VYWIzLxvIAgMBAAGjggHpMIIB5TB0BggrBgEFBQcBAQRoMGYwNgYIKwYB
BQUHMAKGKmh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25lbC5jb20vY2Fyb290LmNydDAsBggrBgEF
BQcwAYYgaHR0cDovL29jc3AuZmlybWFwcm9mZXNpb25lbC5jb20wHQYDVR0OBBYEFIxczJMHb9HV
hmh9gjpB2UwC+JZdMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUZc3rqzUcAD5+1XTA
HLRzRw4aZC8wgcsGA1UdIASBwzCBwDCBvQYEVR0gADCBtDCBsAYIKwYBBQUHAgIwdAxyQ2VydGlm
aWNhZG8gZGUgdXNvIGVuIGh0dHAsLy9d3cuZmlybWFwcm9mZXNpb25lbC5jb20vY3BzMC8GCCsG
aW9uZXMgZGUgdXNvIGVuIGh0dHAsLy9d3cuZmlybWFwcm9mZXNpb25lbC5jb20vY3BzMC8GCCsG
AQUFBwIBFiNodHRwOi8vd3d3LmZpcm1hcHJvZmVzaW9uYWwuY29tL2Nwczs7BgNVHR8ENDAyMDCg
LqAshipodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Zwcm9vdC5jcmwwDgYDVR0PAQH/
BAQDAgEGMA0GCSqGSIb3DQEBCwUAA4ICAQA7REamLqwdXePyP5Wl5kYGEKgtKRZCQGMKKdC0QLwh
XIQLp08lgbEmd5kznsLtgpp4F+mJS7vueWHx1T9ZI0t00Tc7hQzfbGMRtFvjz/wrcSyZ1FYZVOO
JIkUBFpTCCXOMIqXD0YEITANx+Red3F5y4tcTgpWL2t4n7dNiVVwLRGs0MR2lS2a9kMJw6ZE4c+
CMXDR4A19x3Qy8PyQtp772MP79LFUD++qJD7NpSVHGiCsgqJHP28+fiOlBcNunrsCfcQRGr1lFe
B6tk2vj0y6cI2ZEAGrJw6tPRqKMS2jjf2zqeIP8LJmsntJnDyjRNfJVp7YVLEhpJVeKKbGTJvUxm
Hs3nqzdqI374ODyrYLhkhDZp2cxk4bZXGimtrsW4LCRzZet5IVTa7WjW4pa+gMttgFVOwcS6GkZa
5CQokoUE4atKUyBDI74K2BzgKb2UNm6wMqc4g+PsXqoLKu6BpVD5Lp+cup2Ib0lLq3JIX3cvGNRq
8EU3Ncv9Yu9MGy0kTMnJMfPTPECIFqVxU0rQn4/tEY3YYJjplyKow6UjCmWhnRfZMBsEHoD8ukKe
qwacoJW7SbW/b80Vc5QZRLiz7hbQ4hSJ6pu0DNPEC3I5Gn/udfesHQg1aIHacilXjuJlbE94Kpdx
PkBi8CHTM39tIRUkkSPxquBleDUDUnx7Yg==

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

Autoridad de Certificacion Firmaprofesional CIF A62634068

Issuer C:

ES

Subject CN:

AC Firmaprofesional - CUALIFICADOS

Subject SERIAL NUMBER:

A62634068

Subject OU:

Certificados Cualificados

Subject O:

Firmaprofesional S.A.

Subject C:

ES

Valid from:

Fri Dec 14 11:13:23 CET 2018

Valid to:

Tue Dec 31 05:02:00 CET 2030

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:70:89:54:09:A0:9E:D7:68:0C:9C:5B:15:15:E3:DE:F5:9E:76:CE:F7:9B:3F:F2:77:D1:4A:E1:34:7D:07:E2:F9:F2:E9:54:BB:A1:53:9D:F9:A3:10:BE:FA:96:F4:99:93:AD:82:00:D6:2E:F6:8E:9F:13:9D:63:47:AB:44:4D:95:03:33:8D:DF:AE:42:47:95:48:83:AB:A2:14:87:31:E8:DA:87:4C:B1:FB:25:2E:B2:85:83:49:73:9D:84:A5:7E:08:28:CD:FA:7B:DC:08:35:31:25:6F:A3:9A:23:7F:51:56:64:1F:34:11:2B:73:34:71:B4:11:19:13:40:0D:E2:8F:B2:B5:2B:07:4D:36:F0:E8:41:83:23:CE:C4:CE:92:C7:70:48:C5:7C:FC:AF:69:97:5E:D9:45:92:48:2D:55:83:AD:53:CC:F2:4F:83:8C:F9:CE:A6:3C:49:A7:58:BF:AE:1E:9B:8B:E0:C9:73:BD:9F:F5:46:B3:BE:CA:7C:AE:6B:9E:21:1A:48:78:8A:28:ED:D5:AD:CF:79:C8:1D:63:BD:BA:F4:57:E1:96:C2:16:31:29:D7:BC:A3:9E:63:AB:BA:F8:5F:82:92:4C:70:AA:24:4E:E3:1B:C2:11:55:D8:D4:E6:C8:1C:F8:17:38:DD:D5:61:62:33:2F:1B:E5:02:03:01:00:01

Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier

8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D

Basic Constraints

IsCA: true - Path length: 0

Authority Key Identifier

65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points

http://crl.firmaprofesional.com/fproot.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

4C:CF:17:C0:C8:C1:C1:0D:58:76:EC:5E:32:80:FE:8D:13:4D:F3:6A:ED:D8:44:42:89:B9:90:BC:37:41:E7:4F

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description

[en]	*undefined.*
[es]	*undefined.*

Status Starting Time *2019-10-28T01:00:00Z*

17.3.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description

[en]	*undefined.*
[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.13.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.21.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.1.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.11.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.2.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.12.3*

17.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

17.3.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by "AC Firmaprofesional – CUALIFICADOS"*
Name	*[es]*	*Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"*

Service digital identities

X509SubjectName

Subject CN:	*AC Firmaprofesional - CUALIFICADOS*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Cualificados*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *jHHMkwdv0dWGaH2COkHZTAL4ll0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-11-16T00:00:00Z*

17.3.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.13.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.1.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.11.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.2.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.12.3*

17.3.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.3.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

17.3.5 - History instance n.2 - Status: granted

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by "AC Firmaprofesional – CUALIFICADOS"*
Name	*[es]*	*Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"*

Service digital identities

X509SubjectName

Subject CN:	*AC Firmaprofesional - CUALIFICADOS*
Subject SERIAL NUMBER:	*A62634068*
Subject OU:	*Certificados Cualificados*
Subject O:	*Firmaprofesional S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*jHHMkwdv0dWGaH2COkHZTAL4ll0=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

17.3.5.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.10.2*

17.3.5.5 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.1.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.13177.10.1.11.3*

17.3.5.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.3.6 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by "AC Firmaprofesional – CUALIFICADOS"*
Name	*[es]*	*Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"*

Service digital identities

X509SubjectName

Subject CN:	*AC Firmaprofesional - CUALIFICADOS*
Subject SERIAL NUMBER:	*A62634068*

Subject OU: *Certificados Cualificados*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *jHHMkwdv0dWGaH2COkHZTAL4ll0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-07-26T22:00:00Z*

17.3.6.7 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.10.2*

17.4 - Service (granted): AC Firmaprofesional – CLOUD QUALIFIED TSA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *AC Firmaprofesional – CLOUD QUALIFIED TSA*

Name *[es]* *AC Firmaprofesional – CLOUD QUALIFIED TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6161211743113377719*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFnzCCBlegAwIBAgIIVYEFb9Y897cwDQYJKoZIhvcNAQELBQAwgY0xCzAJBgNVBAYTAkVTMR4w
HAYDVQQKDBVGaXJYXBvb2Zlc2lvbmFsIFMuQSAxGjAYBgNVBAsMEVNIY3VyaXR5IFNlcnZpY2Vz
MRIwEAYDVQQFEwlBNjI2MzQwNjgxL1AsBgNVBAMMJUFDIEZpcm1hcHVzZmVzaW9uYWwgLSBJTkZS
QUVTVFJVQ1RVUkEwHhcNMTcwMjI3MTMxOTMzWhcNMjMwMjI2MTMxOTMzWjB2MQswCQYDVQQGEwJF
UzEcMBwGA1UEChMVRmlybWFwcm9mZXNpb25hbCBTLkEuMRgwFgYDVQRhEw9WQVRFUy1BNjI2MzQw
NjgxL TArBgNVBAMTJEZfUk1BUFJPRkVTSU9OQUwgQ0xPVUQgUVVBTEIGSUVEIFRTVTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBALC1poCW9DWDZx/Z6c3z+z6MB1M1S5bLKqXFitYWP95
CTffk5Ai0Uc0E//vRmtwJNfar92fEOT0s3fQe6CUIAkSkFTsMcELmXyYALJmJ28AMa5/wgA0/JcV
N5xoRYWIFF3DZw7NbHODzOatXFwgGIwLP7syWLJXUsY+iQn3zsrm9toillhe68Ki+b7HBIyXk7FN
y5KSs/lc09n7v2lBRhNAsBFcMH6ldYaBb5Kgek9uszF1yP30AgSkc1UTbwdODEUH0Oi8q4WM2pql
Ia5bfGWfstEqPHjJTV7DwaIeDC1ZnoKTzrVC84dMqKc5J55pYSMYqfvNhqwr7zZIMBSICIECAwIEA
AaOCAhcwggITMH0GCCsGAQUFBwEBBHEwbzA/BggrBgEFBQcwAoYzaHR0cDovL2NybC5maXJtYXBy
b2Zlc2lvbmFsLmNvbS9pbmZyYWVzdH11Y3R1cmEuY3J0MCwGCCsGAQUFBzABhiBodHRwOi8vb2Nz
cC5maXJtYXByb2Zlc2lvbmFsLmNvbTAdBgNVHQ4EFgQU8E1CS4ywQL+YYKt7CVQhgcN+7EwDAYD
VR0TAQH/BAIwADAfBgNVHSMEGDAWgBRiFau1swh2pYF+gNk8T8jxH9eTAzBgNVHRAEZzBgQ9v
MDIwMDIyNzEzMTkzM1owfQYDVR0gBHYwdDByBgsrBgEEAcZSCgEEATBjMC8GCCsGAQUFBwIBFiNo
dHRwOi8vd3d3LmZpcm1hcHJvZmVzaW9uYWwuY29tL2NwczAwBggrBgEFBQcCAjAkDCJDZXJ0aWZp
Y2FkbyBkZSBTZXJ2aWNpbyBTZWd1cm8gVFNBMIGABgNVHR8Ez1B3MDmgN6A1hjNodHRwOi8vY3Js
LmZpcm1hcHVzZmVzaW9uYWwuY29tL2luZnJhZXN0cnVydHVvYSSjcmnwwDqA4oDaGNGhbkdHA6Ly9j
cmwyLmZpcm1hcHVzZmVzaW9uYWwuY29tL2luZnJhZXN0cnVydHVvYSSjcmnwwDgYDVR0PAQH/BAQD
AgbAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMA0GCSqGSIb3DQEBCwUAA4IBAQCPFZdNn3BRH+PV
OC6BDe0Ehzw4vXQR8PluEcqjBs//zbwwdsyRZSNQGBJ9bmowOsZge2JTZ2OK84anrHWnY0lZbtcZ
up2ZAecNNyX7X6WKeIjTaHD2cE1OZ27gp1+7Njv1Yg5PX5vs4B4puz3aOAanZEdleADSzpoYH9LX
PJz1ADDESYQWP21TZTC57jAipOAsbtuPdzjYOvcY0L1+9EczTmrsru+PYxgft3ma4Vax37qZj
xtorRxJhYRIEQ9HWT370JSGrUQXdbbC46NF6qhNDiowsG33RUDhXc8hsHqq8L8pmDlH3oXV/YeeZ
0E+vV19ax9lN3AgUc+l9Drrz

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC Firmaprofesional - INFRAESTRUCTURA*

Issuer SERIAL NUMBER: *A62634068*

Issuer OU: *Security Services*

Issuer O: *Firmaprofesional S.A.*

Issuer C: *ES*

Subject CN: *FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Mon Feb 27 14:19:33 CET 2017*

Valid to: *Sun Feb 26 14:19:33 CET 2023*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:B5:A6:80:96:F4:35:83:67:1F:D9:E9:ED:F3:F9:EE:8C:07:53:35:4B:96:CB:2A:A5:C5:8A:D8:98:58:FF:79:09:37:D
F:93:90:22:D1:47:34:13:FF:EF:46:6B:70:24:D7:DA:AF:DD:9F:10:E4:F4:B3:77:D0:7B:A0:94:20:09:12:90:54:EC:31:C1:0B:99:7C:98:00:B2:66:27:6F:00:31:AE:7F:C2:00:34:FC:97:15:37:9C:68:45:85:A5:14:5D:C3:67:0E:CD
:6C:73:83:CC:E6:AD:5C:5C:20:18:8C:0B:3F:BB:32:58:B2:57:52:C6:3E:89:09:F7:CE:CA:E6:F6:DA:22:96:58:5E:EB:C2:A2:F9:BE:C7:04:8C:97:93:B1:4D:CB:92:92:B3:F9:5C:D3:D9:FB:BF:69:41:46:13:40:B0:11:5C:30:7E:
88:75:86:81:6F:92:A0:7A:4F:6E:B3:31:75:C8:FD:F4:02:04:A4:73:55:13:6F:07:4E:0C:45:07:D0:E8:BC:AB:85:8C:DA:9A:A5:95:AE:5B:7C:65:9F:B2:D1:2A:3C:78:E3:4D:5E:C3:BD:A2:1E:0C:2D:59:9E:82:93:CE:B5:42:F3:
88:8C:A8:A7:B9:27:7E:69:61:23:18:A8:8B:CD:86:AC:22:EF:36:49:30:14:A5:08:81:02:03:01:00:01

Authority Info Access

http://crl.firmaprofesional.com/infraestructura.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier *F0:4D:42:4A:5E:32:C1:02:FE:61:82:AD:EC:25:50:86:07:0D:FB:B1*

Basic Constraints *IsCA: false*

Authority Key Identifier *62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79*

Certificate Policies

Policy OID: 1.3.6.1.4.1.13177.10.1.4.1

CPS pointer: http://www.firmaprofesional.com/cps

CPS text: [Certificado de Servicio Seguro TSA]

CRL Distribution Points	*http://crl.firmaprofesional.com/infraestructura.crl* *http://crl2.firmaprofesional.com/infraestructura.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*85:AF:F8:9B:8E:90:39:70:02:70:BB:83:6C:F5:35:8E:B8:85:A9:4F:FA:B4:6E:0E:94:15:F1:6C:5D:21:62:89*

X509SubjectName

Subject CN:	*FIRMAPROFESIONAL CLOUD QUALIFIED TSU*
Subject 2.5.4.97:	*VATES-A62634068*
Subject O:	*Firmaprofesional S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*8E1CSl4ywQL+YYKt7CVQhgcN+7E=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-11-16T00:00:00Z

17.5 - Service (withdrawn): AC Firmaprofesional –INFRAESTRUCTURA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*AC Firmaprofesional –INFRAESTRUCTURA*
Name	*[es]*	*AC Firmaprofesional –INFRAESTRUCTURA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3137071291384231299*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHADCCBOigAwIBAgIIK4kdt/YldYMwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwgQ0lGIEE2
MjYzNDA2ODAeFw0xNTA3MjkxMTI1MDIaFw0zMDEyMzEwNDAyNTVaMIGNMQswCQYDVQQGEwJFUzEe
MBwGA1UECgwYRmNvbWFyYWcmOmZXNpb25lbCBTLkEuIzMRowGAYDVQQLDBFTZWN1cmRlcSBTZXU2aWNl
czESMBAGA1UEBRMJQTYyNjM0MDY4MS4wLAYDVQQDDCVBQyBGaXJtYXBvb2Zlc2vbmFslC0gSU5G
UkFFU1RSVUNUVVJBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuqX7V9RPHmZ/SpGl
hXSfIREtOiiRS8SdJC1QuOB2EYLiFEeL2QFZHIRP4HBm+CbLZ7ts+GLD5XOGWa84Q9BgRI2HXF4E
9PeCQh+cjtnnpDRQIcclkX5zt750xXfjAzifVS4IUHRfivfZmNuyn3qqB5O/nz1KiYelKSZbjo
00qIwXU4sfrZRFJgm0PD6oxJqLoU8VVEjBzdbVWs69KEc91gG0u5UZyLWGJP2f7Uzrk22WOf9S
PfrA01viYw2PSc/81Z7OtADKy076N6Z8ky4HaS1aNsqxx/LTyfUh+9O0ccGKSQSpO87LFbrKNilG
vIRQYzrjItUawGsf0KuUfwIDAQABo4ICnTCCApkwdAYIKwYBBQUHAQEEaDBmMDYGCCsGAQUFBzAC
hipodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Nhcm9vdC5jcnQwLAYIKwYBBQUHMAGG
IGhbdHA6Ly9vY3NwLmZpcm1hcHJvZmVzaW9uYWwuY29tMB0GA1UdDgQWBBRiFau1swh5pYFr+gNki
8178jxH9eTASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFGXN66s1HgA+ftV0wBy0c0cO
GmQvMIIBQQYDVR0gBIIBODCCATQwggEwBgRVHSAAMIIBJjCB8gYIKwYBBQUHAgIwgeUegeIAQwBl
AHIAdABpAGYAaQBjAGEAZABvACAAZABlACAAQQB1AHQAbwByAGkAZABhAGQAIABkAGUAIABDAGUA
cgB0AGkAZgBpAGMAYQBjAGkAbwBuACAAIABDAG8AbgBzAHUAbAB0AGUAIAIBsAGEAcwAgAGMAbwBu
AGQAaQBjAGkAbwBuAGUAcwAgAGQAZQAgAHUAcwBvACAAZQBuACAAaAB0AHQAcAA6AC8ALwB3AHcA
dwAuAGYAaQByAG0AYQBwAHIAbwBmAGUAcwBpAG8AbgBhAGwALgBjAG8AbQAvAGMAcABzMC8GCCsG
AQUFBwIBFiNodHRwOi8vd3d3LmZpcm1hcHJvZmVzaW9uYWwuY29tL2Nwczs7BgNVHR8ENDAyMDCg
LqAshpodHRwOi8vY3hsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Fwcm9vdC5jcmwwDgYDVR0PAQH/
BAQDAgEGMDsGA1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwMGCCsGAQUFBwMI
BggrBgEFBQcDCTANBgkqhkiG9w0BAQsFAAOCAgEAuyL2fYjjyavpt0FzyNnxL/qGfEzl4+Ygf4B1
659KUxv7xxZv4YkttzPVZwz/hf++u80OfwPLsVSqn6nIsnotWqUwk/nInkOu4sEugHDZRn64J2hOv
RULYKSxceSFB6yCPZWWym9dQNBZz+JyWvaBa5NNcNec08EXEkM8+xtO2x/ksxncxShspGLCNgHAvvj
OwuaCGTXikuME5OTPTteNKwJttpgrRk7OEGstDVOM8wQTWSZeZwk3vvc+Oqvb/61jTYCrQi6XhaN
+KcztU4Wgz1F0y11a3qNdZY0VNeLXUsQiCGBb4wpSayBVC6c3ioAc8Xc6kzEcSszLttfUF+oOu7j
fzavDJn9o/oxwtL+nHsHauOY0xMeozrDbKirBiDqra3Qho Wch+Z4GRJKlQqyu63OLkXYz0cQCMs9
d0OAzSeCNVZGEoEM13jOE7oHfV1yAApu1gOvtOqU36HQCz2lA34XHz6+PZybpxokFLvSRQIY
yCtNbdRYkWW0/geV9J65rpx36K0YNDPCNyq35ggf0IAhMT/CBUj/411.9Md0W15y3247LDtU7q
3crNcUEbljH6t1n1ZPC+6w7GGoXQc05gPZo2W5V7Xc0L182+lf62uSJP4fBM54EEoRIe5+anZGfR
z/WDxEbhVTO3MAyg3DvW8B/5vU+K/ihS2XY2CRQ=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - INFRAESTRUCTURA*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Security Services*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Wed Jul 29 13:25:09 CEST 2015*

Valid to: *Tue Dec 31 05:02:55 CET 2030*

Public Key:

```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:A5:FB:57:D4:4F:1E:66:7F:4A:91:A5:85:74:9F:44:41:2D:3A:28:91:4B:C4:9D:24:2D:50:B8:E0:76:11:82:E2:14:47
:8B:D9:01:59:1C:84:4F:E0:70:66:F8:26:CB:67:BB:6C:F8:62:C3:E5:73:86:59:AF:38:43:D0:60:44:8D:87:5C:5E:04:F4:F7:82:42:1F:9E:8E:D9:E7:A4:34:50:97:1F:DC:22:45:F9:CE:DE:F9:D3:15:DF:8C:0A:E2:7D:54:B8:21:41:
D1:7E:2C:9F:66:63:6E:CA:7D:EA:A8:1E:4E:FE:7C:F5:2B:F6:1E:94:A4:99:B5:B8:DC:D3:4A:A5:C1:75:38:B1:FA:D9:44:52:60:9B:43:C3:EA:8C:49:A8:BA:14:F1:55:44:8C:1C:DD:6D:55:AC:1B:D2:84:73:DD:60:1B:4B:B9
:50:96:72:2D:61:89:3F:67:FB:23:FC:EB:92:2D:96:39:FF:52:3D:FA:C0:D3:5B:E2:63:0D:8F:49:EF:FC:D5:9E:CE:B4:00:CA:CB:4E:FA:37:A6:7C:93:2E:07:69:2D:5A:36:CA:B1:C7:F2:D3:CA:55:21:FB:D3:B4:71:C1:8A:49:0
4:A9:3B:CE:CB:15:BA:CA:36:29:46:BC:84:50:63:3A:E3:22:D5:1A:C0:6B:05:D0:AB:94:13:02:03:01:00:01
```

Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier *62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points

http://crl.firmaprofesional.com/fproot.crl

Extended Key Usage

id_kp_clientAuth - id_kp_serverAuth - id_kp_OCSPSigning - id_kp_timeStamping

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

CD:74:19:8D:4C:23:E4:70:1D:EA:57:98:92:32:1B:9E:4F:47:A0:8B:D8:37:47:10:B8:99:AA:D1:49:5A:4B:35

Certificate fields details

Version:

3

Serial Number:

1069733489479276534

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGdTCCBF2gAwIBAgIIDth08OTAV/YwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUF1dG9yaWRhZCBkZSBDZXI0aWZpY2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwgQ0lGIE2
MjYzNDA2ODAeFw0yMDA3MDkxMTEwNTYaFw0zMDEyMzEwNDAyNTYaMIGNMQswCQYDVQQGEwJFUzEc
MBwGA1UECgwVRmlybWFwcm9mZXNpb25hbCBTLkEuMRowGAYDVQQLDBFTZWN1cml0eSBTZXJ2aWNl
czESMBAGA1UEBRMJQTYyNjM0MDY4MS4wLAYDVQQDDCVBQyBGaXJtYXByb2Zlc2lvbmFsIC0gSU5G
UkFFU1RSVUNUVVJBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuqX7V9RPHmZ/SpGl
hXSIREEtOiiRS8SdC1QuOB2EYLrFEcL2QEZHIRP4HB8m+ChLZ7ts+GLD5XOGWa84Q9BgRl2HXF4E
9PeCQh+ejtnnpDRQIs/clkX5zt750xXfjAnfVS4lUHRfiyfZmNuyn3qqB5O/nz1K/YelKSZtbjc
00qlwXU4sfiZRFJgm0PD6oxJqLoU8VVEjBzdbVWsG9KEc91gG0u5UZyLWGJP2f7U/zrki2WOf9S
PfiA01viYw2PSc81Z7OtADKy076N6Z8ky4HaS1aNsqxx/LTyIUh+9O0ccGKSQSpO87LFbrKNilG
vIRQYzrjItUnwGsF0KuUEwIDAQABo4ICFjCCAgswdAYIKwYBBQUHAQEEaD8wMDYGCCsGAQUFBzAC
hipodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Nhcm9vdC5jcnQwLAYIKwYBBQUHMAGG
IGh0dHA6Ly9vY3NwLmZpcm1hcHJvZmVzaW9uYWwuY29tMB0GA1UdDgQWBBRiFau1swh5pYf+gNki
8178jxH9eTASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFGXN66s1HgA+ftV0wByOc0xO
GmOvMIHLBgNVHSAEgcMwgcAwgb0GBFUdIAAwgbQwgYAGCCsGAQUFBwICMHQMcdcNlcnRpZmljYWRv
IGRlIEF1dG9yaWRhZCBkZSBDZXI0aWZpY2FjacOzbi4gQ29uc3VsdGUgbGFzIGNvbmRpY2lvbmVz
IGRlIHVzbyBlbiBodHRwOi8vd3d3LmZpcm1hcHJvZmVzaW9uYWwuY29tL2NwczAvBggrBgEFBQcC
ARYjaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbS9jcHMwOwYDVR0fBDQwMjAwoC6gLIYq
aHR0cDovL2NybC5maXJtYXByb2Zlc2lvbmFsLmNvbS9mcHJvb3QuY3JsMA4GA1UdDwEB/wQEAwIB
BjAnBgNVHSUEIDAeBggrBgEFBQcDAgYIKwYBBQUHAwEGCCsGAQUFBwMIMA0GCSqGSIb3DQEBCwUA
A4ICAQBMPXFyGN5CKTw+kgxWk0Cp4NHfnPxpuTqc+rjI5MqEEnf376l94WZ44gCN5ZWYmKhYWxCc
bpsS/TZ9z5iTFmIbiCLV6RcuUYayzdefKIF9zzli+gdCkFFIUXDUqJBDePX6fE7z89cIALsNH4SG
AKS0fZ8HXOoDOjs1WXI/5IGihhqUAm/a4zh6xfwJpnkB1Rcv0Xc5oK1NSi+1rBcGX33ETcAOlF1ti
dFgmXIbv07wzHQXXrNNTAcqqQgYz0YUo8ab6NNJO/yFNC6o/T0U/Wj5DEX85hTNOB6G+BGbGxTnL
yV25NFKvKteiseM1SrpKf5sXaPGJXsx4XFKaL8wqjBlC33qaETqFBX+aPGgiheWfWFQ+EMthDbVqz
SQjidZKVyzZ0b5q2IyoYK51KzCFV+UMCHyum6UTPPk9RAykVwplfMRaTRGBBbT/SW7Y970nHUwja
iGwra83EAYfOmEEHNcf0A6wHdWgTvvtE7CgDw4jWYTJS41ZcthJO20yKjbYCFdP9pWcF6S8zlPYK
tB8fqoqEpao0PrsJzZD34M0wa3oK0UaqjcI1HXCz0LmBVIbC29SWIeKeEwS6MRw4LoaRuhtpPn
NGaf4LoDxPLYMvPfiuj47CkoS5POkC+Tll6rdZK97YdoQCQuurT/tKV5GGcu3MkhML0Se/LTzZ99
5rplYQ==

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

Autoridad de Certificacion Firmaprofesional CIF A62634068

Issuer C:

ES

Subject CN:

AC Firmaprofesional - INFRAESTRUCTURA

Subject SERIAL NUMBER:

A62634068

Subject OU:

Security Services

Subject O:

Firmaprofesional S.A.

Subject C:

ES

Valid from:

Thu Jul 09 13:10:55 CEST 2020

Valid to:	*Tue Dec 31 05:02:55 CET 2030*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:A5:FB:57:D4:4F:1E:66:7F:4A:91:A5:85:74:9F:44:41:2D:3A:28:91:4B:C4:9D:24:2D:50:B8:E0:76:11:82:E2:14:47:8B:D9:01:59:1C:84:4F:E0:70:66:F8:26:CB:67:BB:6C:F8:62:C3:E5:73:86:59:AF:38:43:D0:60:44:8D:87:5C:5E:04:F4:F7:82:42:1F:9E:8E:D9:E7:A4:34:50:97:1F:DC:22:45:F9:CE:DE:F9:D3:15:DF:8C:0A:E2:7D:54:B8:21:41:D1:7E:2C:9F:66:63:6E:CA:7D:EA:A8:1E:4E:FE:7C:F5:2B:F6:1E:94:A4:99:B5:B8:DC:D3:4A:A5:C1:75:38:B1:FA:D9:44:52:60:9B:43:C3:EA:8C:49:A8:BA:14:F1:55:44:8C:1C:DD:6D:55:AC:1B:D2:84:73:DD:60:1B:4B:B9:50:96:72:2D:61:89:3F:67:FB:23:FC:EB:92:2D:96:39:FF:52:3D:FA:C0:D3:5B:E2:63:0D:8F:49:EF:FC:D5:9E:CE:B4:00:CA:CB:4E:FA:37:A6:7C:93:2E:07:69:2D:5A:36:CA:B1:C7:F2:D3:CA:55:21:FB:D3:B4:71:C1:8A:49:04:A9:3B:CE:CB:15:BA:CA:36:29:46:BC:84:50:63:3A:E3:22:D5:1A:C0:6B:05:D0:AB:94:13:02:03:01:00:01*
Authority Info Access	*http://crl.firmaprofesional.com/caroot.crt* *http://ocsp.firmaprofesional.com*
Subject Key Identifier	*62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]* *CPS pointer: http://www.firmaprofesional.com/cps*
CRL Distribution Points	*http://crl.firmaprofesional.com/fproot.crl*
Extended Key Usage	*id_kp_serverAuth - id_kp_timeStamping*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*84:8C:03:AB:64:7D:5B:D7:E0:D0:C4:3C:0B:5D:67:4C:C9:89:3F:83:6A:B8:63:AF:8F:3F:13:84:B5:44:D8:33*

X509SubjectName

Subject CN:	*AC Firmaprofesional - INFRAESTRUCTURA*
Subject SERIAL NUMBER:	*A62634068*
Subject OU:	*Security Services*
Subject O:	*Firmaprofesional S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*YhWrtbMIeaWH/oDZIvCO/I8R/Xk=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2021-01-26T01:00:00Z*

17.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.5.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *AC Firmaprofesional –INFRAESTRUCTURA*

Name *[es]* *AC Firmaprofesional –INFRAESTRUCTURA*

Service digital identities

X509SubjectName

Subject CN: *AC Firmaprofesional - INFRAESTRUCTURA*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Security Services*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *YhWrtbMIeaWH/oDZIvCO/I8R/Xk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-11-16T00:00:00Z*

17.5.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.6 - Service (granted): Sellos cualificados de tiempo emitidos por FIRMAPROFESIONAL CLOUD QUALIFIED TSU

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos cualificados de tiempo emitidos por FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Name *[en]* *Qualified timestamps issued by FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *150936115047910965630931689977272272981*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFyzCCBLOgAwIBAgIQcY09BY5JQCldWqAi31M1VTANBgkqhkiG9w0BAQsFADCBjTELMAkGA1UE
BhMCRVMxHjAcBgNVBAoMFUZpcm1hcHJvZmVzaW9uYWwgUy5BLjEaMBgGA1UECwwRU2VjdXJpdHkg
U2VydmljZXMxEjAQBgNVBAUTCUE2MjYzNDA2ODEuMCwGA1UEAwwIQUMgRmlybWFwcm9mZXNpb25h
bCAtIE1RUBRVNlUlVDVFVSQTAeFwfyMDAyMDYwOTM5MTNaFwfyNjAyMDQwOTM5MTNaMHYxC2AJ
BgNVBAYTAkVTMR4wHAYDVQQKExVGaXJtYXByb2Zlc2lvbmFsIFMuQS4xGDAWBgNVBGETD1ZBVEVT
LUE2MjYzNDA2ODEtMCsGA1UExxMkRklSTUFQUk9GRVNJT05BTCBDTE9VRCBRVUFMSUZJRUQgVFNV
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAIWgXHdXrx07wJBaZv97KvmSR/LR2fA6D
V/FtCFI8OXBI/+DWnWcgbG1IuIRTnJE+3bfU/XRRPVFnEnVkn3HY69guUYYHWiCgnqkBzXUnsbX7LS
vTbPcd7GXtB9XZD3RP+i7ftnePMZYbt+QxNDL3lFg5fTHbKt+1vsOrdbzKktpSs20iXfEQwm1JR
AcVibgt+8AbKMoRf2DjlU/GpAnLW4Eo6398rtkQm63S646vkUncJA3UW6lYrbH8/sdvpkT6Nn2Xzz
bEYb6Allnx/cuxx/sU/+Wnaw6YdaS+DJMY5smprHbmhRJZDadbD6vgHRj4tLbZIQFRs1JowpCT8OD
ozutfisIDAQABo4ICOzCCAjcwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRiFau1swb5pYf+gNki
8178jxH9eTB9BggrBgEFBQcBAQRxMG8wPwYIKwYBBQUHMAKGM2h0dHA6Ly9jcmwuZmlybWFwcm9m
ZXNpb25hbC5jb20vaW5mcmFlc3RydWN0dXJhLmNydDAsBggrBgEFBQcwAYYgaHR0cDovL29jc3Au
ZmlybWFwcm9mZXNpb25hbC5jb20wgY8GA1UdIASBhzCBhDCBgQYLKwYBBAHmeQoBBAEwcjAvBggr
BgEFBQcCARYjaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbS9jcHMwPwYIKwYBBQUHAgIw
MwwxQ2VydGlmaWNhZG8gZGUgU2VydmljaW8gU2VndXJvIGRlIFTQSBjdWFsaWZpY2FkYTAWBgNV
HSUBAf8EDDAKBggrBgEFBQcDCDCBgAYDVR0fBHkwdzA5oDegNYYzaHR0cDovL2NybC5maXJtYXBy
b2Zlc2lvbmFsLmNvbS9pbmZyYWVzdHU1Y3R1cmEuY3JsMDggOKA2hjRodHRwOi8vY3JsMi5maXJt
YXByb2Zlc2lvbmFsLmNvbS9pbmZyYWVzdHU1Y3R1cmEuY3JsMB0GA1UdDgQWBBRpGW3lKQCVrG3o
SKa3moxZgn2nczArBgNVHRAEJDAigA8yMDIwMDIwNjA5MzkxM1qBDzIwMjMwMjAiMDkzOTEzWjAO
BgNVHQ8BAf8EBAMCBsAwDQYJKoZIhvcNAQELBQADggEBAE2lPaUWJvFvWQyZrg4IvwOx2mSM6sla
7Zs2/7oJ0b0UGcFOEHAE3yLally95TLbzO1Uj+MDJ31EgbpOEUGVLN1lCgMkFWNA275+y4SHQQT
oUiCuXeQwewyC5nw/u5BiVd4UlhEiL1A2g45r0oWJ21l8uQj2Nd4pXNtu5JApB7fXK2vs1yQGOo/2
8JfcF09gHD1D0IVTnko0Wstjk1ZZIedgRMb7oMS4hBf4QnIPpHcSTBiHDAZTTQDCtNKCJgt63NBVh
JGbnxYfa+T+ixV034ARMqRAeIioyfKjjVkRtgW7arLCA0ZPGa+VF3HWH41a9CYKpF9WknPese6/M
tuA4XbE=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC Firmaprofesional - INFRAESTRUCTURA*

Issuer SERIAL NUMBER: *A62634068*

Issuer OU: *Security Services*

Issuer O: *Firmaprofesional S.A.*

Issuer C: *ES*

Subject CN: *FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C:	*ES*
Valid from:	*Thu Feb 06 10:39:13 CET 2020*
Valid to:	*Wed Feb 04 10:39:13 CET 2026*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:95:68:17:1D:D5:EB:C7:4E:F0:24:16:99:BF:DE:CA:BE:64:91:FC:B4:76:7C:0E:83:57:F1:6D:08:52:3C:39:70:54:F8:35:A7:59:E8:DB:1B:52:2E:25:14:E7:24:4F:B7:6D:F5:17:45:13:D5:16:71:27:56:49:F7:1D:8E:BD:82:25:18:60:75:A2:0A:09:EA:90:1C:D7:52:7B:1B:5F:B2:D2:BD:36:CF:71:DE:C6:5E:D0:7D:5D:90:F7:44:FF:A2:ED:FB:67:78:F3:19:61:BB:7E:43:13:43:2F:79:45:83:97:D3:1D:B2:AD:FB:5B:EC:3A:B7:5B:CC:A9:2D:A5:2B:36:D2:25:DF:11:0C:26:D7:52:51:01:C5:62:6E:0B:7E:F0:06:CA:32:84:5F:D8:38:E5:50:6A:40:9C:B5:B8:12:8E:B7:F7:CA:ED:91:09:BA:DD:2E:B8:EA:F9:14:9D:C2:40:DD:45:BA:95:8A:DB:1F:CF:EC:76:FA:64:4F:A3:67:D9:7C:F3:6C:46:15:E8:09:65:9F:1F:DC:BB:1C:7F:B1:4F:96:9D:AC:3A:61:D6:92:F8:32:4C:63:9B:26:A6:B1:DB:9A:14:49:64:36:9D:6C:3E:AF:80:74:63:E2:D2:DB:66:54:05:46:CD:49:A3:0A:42:4F:C3:83:A3:3B:AD:7F:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79*
Authority Info Access	*http://crl.firmaprofesional.com/infraestructura.crt* *http://ocsp.firmaprofesional.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.13177.10.1.4.1* *CPS pointer: http://www.firmaprofesional.com/cps* *CPS text: [Certificado de Servicio Seguro de TSA cualificada]*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://crl.firmaprofesional.com/infraestructura.crl* *http://crl2.firmaprofesional.com/infraestructura.crl*
Subject Key Identifier	*69:19:6D:E5:29:00:95:AC:6D:E8:48:A6:B7:9A:8C:59:82:9D:A7:73*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*CC:93:E2:7B:3D:2B:C8:FF:4E:4D:0E:65:2F:A2:18:7F:E3:AB:5D:FA:65:28:72:5C:FE:E3:70:E0:79:9C:E1:4A*

X509SubjectName

Subject CN:	*FIRMAPROFESIONAL CLOUD QUALIFIED TSU*
Subject 2.5.4.97:	*VATES-A62634068*
Subject O:	*Firmaprofesional S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*aRlt5SkAlaxt6Eimt5qMWYKdp3M=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

	[es]	*undefined.*

Status Starting Time *2020-04-28T00:00:00Z*

17.7 - Service (granted): Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2020

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2020*
Name	*[es]*	*Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2020*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *133529187700912422781168782320038630024*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGeTCCBGGgAwIBAgIQZHTJPiF08nD3crsRjhjSiDANBgkqhkiG9w0BAQsFADBRMQswCQYDVQQG
EwJFUzFCMEAGA1UEAww5QXV0b3JpZGFkIGRlIENlcnRpZmlyYWNpb24gRmlybWFwcm9mZXNpb25h
bCBDSUYgQTYyNjM0MDY4MB4XDTIwMDczMDA4NTgxNFoXDTIzMDczMDA4NTgxNFowgZMxCzAJBgNV
BAYTAkVTMR4wHAYDVQQKDBVGaXJtYXByb2Zlc2lvbmFsIFMuQS4xGDAWBgNVBGEMD1ZBVEVTLUE2
MjYzNDA2ODEaMBgGA1UECwwRU2VjdXJpdHkgU2VydmlpZXMxLjAsBgNVBAMMIUFDIEZpcm1hcHUv
ZmVzaW9uYWwgLSBTZWN1cmUgV2VilDIwMjAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQC+Hm7Qfe1jfkti/zTjd4pPkXaOQrxLAHCNXrI+nnW1PQ3wUS7kjJZR5lM5adcUaBhiKZqk6m
PbZSSwNiASyOVdV4j5OW617CkGbaFNdct3yOvWCnECCnlOQVNj8Ps+QZpsPTEQTaDixozKaVwiGq
fypOvzU9jBtmQ28YnQAuZqNQwGKusSCV9FI55OzZbQDNqOLbU5z0IIPMyEi1SW0e7IuIMBXLtZ8
P8nG0qFbaBhmWX9+Lmeku30UXGd/meVN1u5I/5TRGvsFOsDzus82NCHgqqa69kF0dmrLNcN+oHRp
bRPESQ+IQZG3ls6/kaHucDRW5dRDoVjWWlfITAzAgMBAAGjggIlMIICBD80BggrBgEFBQcBAQRo
MGYwNgYIKwYBBQUHMAKGKmh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20vY2Fyb290LmNy
dDAxBggrBgEFBQcwAYYgaHR0cDovL29jc3Auem1yb WFwcm9mZXNpb25hbC5jb20wHQYDVR0OBBYE
FL2XDmelaO0pG5uragqKNoqNLbYpMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUZc3r
qzUeAD5+1XTAHLRzRw4aZC8wgcsGA1UdIASBwzCBwDCBvQYEVR0gADCBtDCBgAYIKwYBBQUHAgIw
dAxyQ2VydGilmaWNhZG8gZGUgQXV0b3JpZGFkIGRlIENlcnRpZmlyYWNpw7NuLiBDb25zdWx0ZSBs
YXMgY29uZGIjaW9uZXMgZGUgdXNvIGYuIGibddHA6L y93d5cuZmlybWFwcm9mZXNpb25hbC5jb20v
Y3BzMC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LmZpcm1hcHJvZmVzaW9uYWwuY29tL2NwczA7BgNV
HR8ENDAyMDCgLqAshipodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Zwcm9vdC5jcmww
DgYDVR0PAQH/BAQDAgEGMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATANBgkqhkiG9w0B
AQsFAAOCAgEAoBcsiFUrycuyAphpdbhavefqWDQjeNyG4FplrBNMjRPRNhl8KOqAKlqCcw0YNleb
/wsF9QAO0FK4NRPc+Ett8lCGhZGV/F/QNanlovbRqqqIL Itapb4AI2owITDulq7 91P8kD+tiMfvnq
skwLzyznjBm8c6f20NCE1qRTZCoauAa7IoMBVwIV+K/fLWRCH4/hA/YjSlZ6IzwFQ7Z4ZVmSBZud
QxevaRAH43gm1GsufoOzcB3qHIY510KplpmHZmiobx58P3nxLKAaVNu3WVfkgNcWYzeo8PD3JV+Q
KSa97MdLJN4D7EdKiwyVn8gJtiUmC6Pi35e5DcyHmvnTD91yNxE8bHb6TjZtQq6Fn0SzA 7oktn
sFmcGjbl4oE0mMp85444b5RPpIuKnBF+7QZSs1dz9lUVRmvk1bMDt5gPnXDnu0tc2FLWZKi2dvAEv
eBWUmrMAtGts5bJHclHLsBmK TJSS9aME/CHY95Q/qXSPx+djY4/4+Ti30AlZLUel+NhX2qtPje4f
6g6pMiTPHN8RNbiwQPPscTCl8vPk8SBBg9rTDl7WQFeqfwr8QWeTavSjIxM3htacv4xqKXayFEu
I2+MIYt8ikNwZrghLY4Zv+BY4b+CxWIt9W9c5hu4Jel0NHFyGXPeutUS3bXJW+NS7ohcLFzoxvt56
h6XAhEkqeAc=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - Secure Web 2020*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Thu Jul 30 10:58:14 CEST 2020*

Valid to: *Sun Jul 30 10:58:14 CEST 2023*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BE:1E:6E:D0:7D:E5:23:7E:4B:62:FF:34:E3:77:8A:4F:91:76:8E:42:BC:4B:00:70:8D:5E:B9:7E:9E:75:B5:3D:0D:F0:51:2E:FF:92:32:59:47:92:0C:E5:A7:5C:94:96:81:6E:22:99:AA:4E:A6:3D:BD:92:4B:03:62:01:2C:8E:55:D5:78:8F:93:96:EB:5E:C2:90:66:DA:14:D7:5C:B7:7C:8E:BD:60:A7:10:20:A7:20:E4:15:36:3F:0F:B3:E4:19:A6:C3:D3:11:04:DA:0E:2C:68:CC:A6:95:C2:21:AA:7E:FA:4E:BF:35:3D:8C:19:90:D9:16:27:40:08:99:A8:D4:30:18:AB:AC:E4:25:7D:14:8E:79:3B:36:5B:40:33:6A:FC:E2:DB:53:9C:F4:7C:83:CC:C8:48:B5:49:6D:28:EC:9B:88:30:15:CB:B4:9D:BC:3E:C9:C6:D2:A1:5B:68:18:66:59:7F:7E:2E:67:A4:BB:7D:14:5C:67:7F:99:E5:4D:D6:EE:65:FF:94:D1:1A:FB:05:3A:C0:F3:BA:CF:36:34:21:E0:AA:A6:BA:F6:41:74:76:6A:CB:35:C3:7E:A0:74:69:6D:13:C4:E5:0F:A5:41:91:B7:96:CE:BF:91:A7:E5:B9:C0:D1:5B:97:51:0E:85:63:59:69:5F:95:30:33:02:03:01:00:01*

Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier *BD:97:0E:67:88:68:ED:29:1B:9B:AB:6A:0A:8A:36:8A:8D:2E:16:29*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Extended Key Usage *id_kp_serverAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *93:3B:80:F7:B9:72:55:DF:5C:F1:D9:5A:12:3E:90:17:22:DD:B3:0B:48:1A:F3:AA:83:54:82:01:11:9E:D3:03*

X509SubjectName

Subject CN: *AC Firmaprofesional - Secure Web 2020*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *vZcOZ4ho7Skbm6tqCoo2io0uFik=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

17.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.8 - Service (granted): AC Firmaprofesional CLOUD QUALIFIED TSU-2020

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *AC Firmaprofesional CLOUD QUALIFIED TSU-2020*

Name *[es]* *AC Firmaprofesional CLOUD QUALIFIED TSU-2020*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *96352306425787635861384208292947363613*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFIDCCBHygAwIBAgIQSHzHeqzECoxpP5jU8hcHHTANBgkqhkiG9w0BAQsFADCBkjELMAkGA1UE
BhMCRVMxHjAcBgNVBAoTFUZpcm1hcHJvZmVzaW9uYWwgUy5BLjEiMCAGA1UECxMZQ2VydGlmaWNh
ZG9zIEN1YWxpZmlpYWRvczESMBAGA1UEBRMJQTYyNjM0MDY4MSswKQYDVQQDEyJBQyBGaXhYXBy
b2Zlc2lvbmFslC0gQ1VBTEIGSUNBRE9TMBAXDTIwMDgwNjExMzkzM1oXDTI2MDgwNTExMzkzM1ow
fTELMAkGA1UEBhMCRVMxHjAcBgNVBAoMFUZpcm1hcHJvZmVzaW9uYWwgUy5BLjEYMBYGA1UEYQwP
VkFURVMtQTYyNjM0MDY4MTQwMgYDVQQDDCtGSVJNQVBST0ZFU0lPTkFMIENMT1VEIFFVQUxJRkIF
RCBUU1UgLSAyMDIwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoQEoKGFNMCPXE63n
6bpveHomzkzFGKnG11XdCYqANFuqkVjfTNkth8XIqItnbC8cAZaWS/umvzld7BzQMjuXRz3y6Fx
gRwIF6fO1u30t/cap5KurYon+83kNT8EDTdMnFD2HWstOtSwIARWDZIuWZgYimYXtkLMGLpMWF+
EU9NCSwCXmnSRVbGQkCsLwzVW0q6QiFON5uG2fmKJlodtEckQdEdlRDUiTemVIo6Xkypgz/pA6q
FcLyDkJUyJeHHx9DRhAjpXm1aZfEW0CYeUOrZ7MnrUuA++foc0TNlFyR4g5sM6osJ3QoA13VZj
RsytesdjfSKGQ+6MJMOaQIDAQABo4IB+DCCAfQwDAYDVR0TAQH/BAIwADADBgNVHSME GDAWgBSM
ccyTB2/R1YZofYI6QdlMAvrWXTB6BggrBgEFBQcBAQRuMGwwPAYIKwYBBQUHMAKGMGh0dHA6Ly9j
cmwuZmlybWFwcm9mZXNpb25hbC5jb20vY3VhbGlmaWNhZG9zLmNydDAsBggrBgEFBQcwAYYgaHR0
cDovL29jc3AuZmlybWFwcm9mZXNpb25hbC5jb20wgY8GA1UdIASBhzCBhDCBgQYLKwYBBAHmeQoB
BAEwcjAvBggrBgEFBQcCARYjaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbS9pcHMvaPwY1
KwYBBQUHAgIwMwwxQ2VydGlmaWNhZG8gZGUgU2VydmljaW8gU2VndXJvIGRlIFRTQSBjdWFsaWZp
Y2FkYTAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vY3Js
LmZpcm1hcHJvZmVzaW9uYWwuY29tL2N1YWxpZmlpYWRvcy5jcmwwHQYDVR0OBBYEFP17RQ7pgAL9
PutVqr4lZvdPIVWMCsGA1UdEAQkMCKAD2xlwMjAwODA2MTEzOTMzWoEPMjAyMzA4MDYxMTM5MzNa
MA4GA1UdDwEB/wQEAwIGwDANBgkqhkiG9w0BAQsFAAOCAQEADbZdD6Uvs5Tu8x1P0blCksSLSbln
QDtnNsiOaPFDIfgZwIeGwD+339mAjlSCUetsDWVM6iTmnM8BPlPWo/YoZqDDqMYhcrbKSBPYCPn
jTTrzouXdWRMLMupCB4zZyJCoy6VIMjTCCMj+z5DtBwIzpelXlArDZkQrNtmLbyTfeYyA/83y7D+
Y96ZARuUVYbiRoHPyXIVakd7TWWr6BbbwCuU2prLZ6fbOapZtaKZjROrN28QyPnVYRuOTiCM
bLZk25zTYY5z1lXDWvjf2/oNopn+nyWrb97Ha3zBq9t/O0aoJ1J++d3bvX8ICsk3V+thI/cfALYu
YtmeMhKCjg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC Firmaprofesional - CUALIFICADOS*

Issuer SERIAL NUMBER:	*A62634068*
Issuer OU:	*Certificados Cualificados*
Issuer O:	*Firmaprofesional S.A.*
Issuer C:	*ES*
Subject CN:	*FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020*
Subject 2.5.4.97:	*VATES-A62634068*
Subject O:	*Firmaprofesional S.A.*
Subject C:	*ES*
Valid from:	*Thu Aug 06 13:39:33 CEST 2020*
Valid to:	*Wed Aug 05 13:39:33 CEST 2026*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A1:01:28:28:61:4D:30:23:D7:13:AD:E7:E9:BA:6F:78:7A:22:9B:39:33:14:62:A7:1B:5D:57:74:26:2A:00:D1:6E:AA:45:63:7D:33:64:B6:1F:17:22:A2:2D:9D:B0:BC:70:06:5A:5B:9F:EE:9A:FC:E5:77:B0:73:40:C8:EE:5D:1C:C9:CB:A1:71:81:1C:35:17:A7:CE:D6:ED:F4:B7:F7:1A:A7:92:AE:AD:8A:27:FB:CD:E4:35:3F:04:0D:37:4C:AE:21:43:D8:75:AC:B4:EB:52:C0:80:11:58:36:48:B9:66:60:62:29:98:5D:F9:0B:30:62:E9:31:61:7E:11:4F:4D:09:2C:02:5E:69:D2:45:56:C6:42:40:AC:2F:0C:D5:5B:4A:BA:95:08:85:38:DE:6E:1B:67:E6:28:99:68:76:D1:1C:91:07:44:75:F4:43:52:24:DE:99:52:28:E9:79:32:A6:0C:FF:A4:0E:AA:15:C2:F2:0E:42:54:C8:97:87:16:1C:7D:0D:16:C0:8E:95:E6:8B:56:99:7C:45:8E:0B:D7:94:3A:B6:7B:32:7A:D4:B8:0F:BE:7E:87:34:4C:D9:45:C9:1E:20:E6:C3:3A:A2:C2:77:42:20:35:DD:56:63:46:CC:AD:7A:F7:5F:8C:5E:4A:19:0F:BA:30:93:0E:69:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*
Authority Info Access	*http://crl.firmaprofesional.com/cualificados.crt* *http://ocsp.firmaprofesional.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.13177.10.1.4.1* *CPS pointer: http://www.firmaprofesional.com/cps* *CPS text: [Certificado de Servicio Seguro de TSA cualificada]*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://crl.firmaprofesional.com/cualificados.crl*
Subject Key Identifier	*FD:7B:45:0E:E9:80:02:FD:3E:EB:55:8A:AA:C8:E1:9B:DD:3F:55:56*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*E9:F0:94:3D:FC:4D:49:33:39:62:8A:18:3B:1F:89:09:B4:FD:B8:7B:C1:D9:1B:0C:BC:D1:7B:F3:83:3C:20:22*

X509SubjectName

Subject CN:	*FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I */XtFDumAAv0+61WKqsjhm90/VVY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

17.9 - Service (granted): Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2021

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2021*

Name *[es]* *Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2021*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *118834116822395291903889089598114208304*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGeTCCBGGgAwIBAgIQWWacT3uC/Pmrj1Y4QbOaMDANBgkqhkiG9w0BAQsFADBRMQswCQYDVQQG
EwJFUzFCMEAGA1UEAww5QXV0b3JpZGFkIGRlIENlcnRpZmlfYWNpb24gRmlybWFwcm9mZXNpb25h
bCBDSUYgQTYyNjM0MDY4MB4XDTIxMDMwNTEwNDMzNVoXDTI0MDMwNDEwNDMzNVowgZMxCzAJBgNV
BAYTAkVTMR4wHAYDVQQKDBVGaXJtYXByb2Zlc2lvbmFsIFMuQS4xGDAWBgNVBGEMD1ZBVEVTLUE2
MjYzNDA2ODEaMBgGA1UECwwRU2VpdXJpdHkgU2VlYvdmIjZXMxLjAsBgNVBAMMIUFDIEZpcm1hcHIr
ZmVzaW9uYWwgLSBTZWN1cmUgV2ViIDIwMjEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCiluCxxUz5be+4L56w0MloHgYTz3GGjMXwpOxHWUUllw0O94J22/BIXXjsJjbfLthnRzJ19C8m
a4NhmhZTDwHkA/Zq1IjgYXfEMwRML8uL2IOxSfAXJFJs1FNoaCtf3dhxcbrcPu/pj0jSbF6XoZrD
LhnchI-4jqqC7L59MBfZ8QfKJTJ0JExrOR/RrUdXGiZuLxLmhkvSqu1HCaNjwcjfAD9r2bf73DY
ciaql52KZKfuXPUGUFvtTmiB3YqDo8bVciFySAY2N8GGqzf7l8NAcjRy6hpNvHBwCIW+OFNbGce
T6AYdVibd0mT1RFpd9i6+zdvpzMAAdyD/xJcPNXAgMBAAGjggIIMIICBDB0BggrBgEFBQcBAQRo
MGYwNgYIKwYBBQUHMAKGKmh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20vY2Fyb290LmNy
dDAsBggrBgEFBQcwAYYgaHR0cDovL2Fjc3AuZmlybWFwcm9mZXNpb25hbC5jb20vMjAyMDcwMDcw
FAYJOhyqCBtOtc3WW5KK3N3nxvMBIGA1UdEwEBwQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUZc3r
qzUcAD5+1XTAHLRzRw4aZC8wgcsGA1UdIASBwzCBwDCBvQYEVR0gADCBtDCBgAYIKwYBBQUHAgIw
dAxyQ2VydGlmaWNhZG8gZGUgQXV0b3JpZGFkIGRlIENlcnRpZmlfYWNpw7NuLiBDb25zdWx0ZSBs
YXMgY29uZGlja W9uZXMgZGUgdXNvIGVuIGh0dHA6Ly93d5cuZmlybWFwcm9mZXNpb25hbC5jb20v
Y3BzMC8GCCsGAQUFBwIBFiNodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Nwczs7BgNV
HR8ENDAyMDCgLqAshipodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Zwcm9vdC5jcmww
DgYDVR0PAQH/BAQDAgEGMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATANBgkqhkiG9w0B
AQsFAAOCAgEARvzsXuC3erAdhsY++QEV3iMwC+kk7qOwRcnj5hMAGV3KArI3jBI1nMSTefmPqUU
UPPj4TbNDHoXzjZzeIrFFtEtE/Mxs9rZkXMnR+qwBKTZ9o6n1IrzrqXdTzN+jdflNbRcGedBzeG
lqTz1S9+cdJ76KsDjjZb3HoH0iSPtSqTgYi+bzyFgAyoDB1awjw5h341oGtQ0nmijQ1ySfRr35W
Ws2DOtI2rq6GDlapZBWZzCGcwfI5JblwagDRFS037dlLz8VqJb2r8W9NtfAiAydzEh2FEbBU2uWj
vgu/a24V5ggeYtIL WoCxBqPxd7+eqt4KQRnyesD69czzZuGg/cHaQSZ100X0XLzDMY3ScRT6e4k4
BPf8oSsYXuYoB9nvWNXEzkJUSFqXPfEDH(2cgFKpocbBE/CYpyMb4IEAON/OumGsVjaUdlG/RxLSX
Uw1U4VBUQ8kYE8t+UnaKwozAav5VxDgzs+7Wx1zdJBDGh2vXGXQasCy0JtQwQC+8Jn9bDB8cawcQ
GLQ/WaYInbGC/W8e003aDYz3s+lBSKed31IPxEAqVYConQkCGRwquGxLxD7pEjpw4N+4YUvkW8BT
ilxZ2L6cGBTimGGcOMDV4Z60C1plcRjSCTIIzHLYHAhEVt/M995WRs/9oxITjzhHunHnBDTLnnNe
eYTHn+VOalo=

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Autoridad de Certificacion Firmaprofesional CIF A62634068*
Issuer C:	*ES*
Subject CN:	*AC Firmaprofesional - Secure Web 2021*
Subject OU:	*Security Services*
Subject 2.5.4.97:	*VATES-A62634068*
Subject O:	*Firmaprofesional S.A.*
Subject C:	*ES*
Valid from:	*Fri Mar 05 11:43:35 CET 2021*
Valid to:	*Mon Mar 04 11:43:35 CET 2024*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A2:96:E0:B1:C5:4C:F9:6D:EF:B8:2F:9E:B0:D0:C2:28:1E:06:13:CF:71:86:8C:C5:F0:A4:EC:47:59:45:08:97:0D:0E:F7:82:76:DB:F0:48:5D:78:EC:26:36:DF:2E:D8:67:47:32:75:F4:2F:26:6B:83:61:9A:16:53:0F:01:E4:03:F6:6A:23:58:E0:61:77:C4:33:04:4C:2F:CB:8B:D8:93:B1:49:F0:17:24:52:6C:D4:53:68:68:2B:5F:DD:D8:71:71:BA:DC:3E:EF:E9:8F:48:D2:6C:5E:97:A1:9A:C3:2E:19:DC:6C:BE:23:AA:A0:BB:2F:9F:78:06:D6:7C:41:F2:89:EC:98:D0:13:1A:CE:47:F4:6B:53:F7:57:B4:68:99:B8:BC:4B:9A:19:2F:4A:AB:B5:1C:26:8D:8F:07:23:7C:00:FD:B7:66:E5:EF:70:D8:7A:26:AA:23:9D:8A:64:A7:EE:5C:F5:06:50:5B:ED:4E:68:81:DD:8A:83:A3:C6:D5:72:21:72:48:06:36:37:C1:86:AB:37:FB:97:C3:40:72:34:72:EA:1A:4D:BD:F1:C1:C0:29:56:F8:E1:4D:6C:67:1E:4F:A0:18:75:58:9B:77:49:93:D5:11:69:77:D8:BA:FB:37:6F:A7:33:00:01:D8:B2:0F:FC:49:78:F3:57:02:03:01:00:01*
Authority Info Access	*http://crl.firmaprofesional.com/caroot.crt* *http://ocsp.firmaprofesional.com*
Subject Key Identifier	*0B:6A:EC:EB:B2:A8:20:6B:3A:D7:B7:59:6E:4A:2A:2D:CD:DE:7C:6F*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]* *CPS pointer: http://www.firmaprofesional.com/cps*
CRL Distribution Points	*http://crl.firmaprofesional.com/fproot.crl*
Extended Key Usage	*id_kp_serverAuth*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*59:22:85:35:D1:14:E8:D2:9F:9B:92:D4:22:51:8B:C6:3D:DC:B5:70:97:42:8D:8C:C9:87:77:D9:07:C6:EE:FE*

X509SubjectName

Subject CN: *AC Firmaprofesional - Secure Web 2021*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *C2rs67KoIGs617dZbkoqLc3efG8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-03-17T01:00:00Z*

17.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.10 - Service (granted): Qualified timestamps issued by “AC Firmaprofesional Timestamp 2021"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by “AC Firmaprofesional Timestamp 2021"*

Name *[es]* *Sellos cualificados de tiempo emitidos por “AC Firmaprofesional Timestamp 2021"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *115136804081726244375824872832178605 48*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHbjCCBVagAwIBAgIQCKl0RZZkBnLN0iICYhYHxDANBgkqhkiG9w0BAQsFADBRMQswCQYDVQQG
EwJFUzFCMEAGA1UEAwwSQXV0b3JpZGFkZGRlIENlcnRpZmlyYWNpb24gRmlybWFwcm9mZXNpb25b
bCBDSUYgQTYyNjM0MDY4MB4XDTIxMDQxMzA5MzIyMFoXDTMwMTIzMTA0MDIwMFowgZIxCzAJBgNV
BAYTAkVTMR4wHAYDVQQKDBVGaXJtYXByb2Zlc2lvbmFsIFMtQS4xGDAWBgNVBGEMD1ZBVEVTLUE2
MjYzNDA2ODEaMBgGA1UECwwRU2VjdXJpdHkgU2VydmljZXMxLTAzBgNVBAMMIEFDIEZpcm1hcHJv
ZmVzaW9uYWwgLSBUaW1lc3RhbXAgMjAyMTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
AM0InM0FIG1/0W05AEYe5ytfaIVWUqwgsAgy6uPUuq3WD24yDBz2mizS9tsiDi/WSzN5QwHh7ql/9
4q08hTKJwY6a60QRKxHEmxvGbvAmoCbvqsjb+ELGOVKwGazQyugjGOEq97d6Dg33uW5icRJatL1J
63h3gmraVcakSMIvPF90CDwm+8d3bnFakjPZju88gLXTwOdAoNwELsQRdQQ1viNEcit3vAuODMbO
t9zdIjObvNcS6yVJFidcA6GFvBbnm9Oq9mBwn9PBLSTwxbepl13wrNPkXydBCo80IfzvZFInI3
Pp7yf7X4UPQmA6sWi30uWqYR7BUL9DI6fzATxzYKbEp9DZmoR72kA9SYHv+9M7r6cXUA2Ypwda9
LxRS6zzLB50bT8nPto1Fcr7FwNP2ESqVh3U2WZT3XCTluMxD6en4TQWwPqX+7skWRv6TU2mp4Xk2
WJmVn8KTBSlpSO67QgCLTI43iGcBFVoZAdTgxIL9AmrZEGXMgvpi98NosPGnUY2RoWpSmZ6vxhuD
SgVNsuUzuzlb2V77l7cHaregs401CFginEaBsQvHUp7ggSs+mNDwqtdPGPcQGSx0SiGuw8VI7sa4
UeDXvLq8VjRmg5L77lZFTLpB4YoE1VbXfbbMnS9yCYgc2SOLsPbnRO+pKs6ifkRwRBkRtgP
AgMBAAGjggH+MIIB+jASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFGXN66s1HgA+ftV0
wBy0c0cOGmQvMHQGCCsGAQUFBwEBBGgwZjA2BggrBgEFBQcwAoYqaHR0cDovL2NybCSmaXJtYXBy
b2Zlc2lvbmFsLmNvbS9jYXJvb3QuY3J0MCwGCCsGAQUFBzABhiBodHRwOi8vb2Nzcc5maXJtYXBy
b2Zlc2lvbmFsLmNvbTCBywYDVR0gBIHDMIHAMIG9BgRVHSAAMIG0MIGABggrBgEFBQcCAjB0DHID
ZXJ0aWZpY2FkbyBkZSBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2nDs24uIENvbnN1bHRlIGxhcyBj
b25kaWNpb25lcyBkZSB1c28gZW4gaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbS9jcHMw
LwY1KwYBBQUHAgEWI2h0dHA6Ly93d3cuZmlybWFwcm9mZXNpb25hbC5jb20vY3BzMBMGA1UdJQQM
MAoGCCsGAQUFBwMIMDcGA1UdHwQ0MDIwMKAuoCyGKmhldHA6Ly9jcmwuZmlybWFwcm9mZXNpb25h
bC5jb20vZnByb290LmNybDAdBgNVHQ4EFgQUFqat6WzF2984R0wavEY2WN4s62IuDgYDVR0PAQH/
BAQDAgEGMA0GCSqGSIb3DQEBCwUAA4ICAQBrLOh9OoFZDbxdPrP2DSj7K6+i+++n2RaZXloMGykX
PZYRBZlDpakO3JPqxMBoCUyRqRJXaKifMSxmLURnaN3F0o4mEIO9BqVfpJeQCF4sElBTyIRVs72N
UyGFf4ZGlEWTqVFwOtPUsI2zkcUNkzhIY/212CC07Wu6ajQa/B3fK6C1aU0MPuhI0rF8tQSEUiB6
fIZ7IPlcGWbSZuKKGw0NC14OhdN0jOACombRtb+7EFlKPAcc81sX/S2su6gsKpNITZnY89mxHL
9/guegGkr6M+V3c3Bw9Ks3Uy1TgIshHprI73dOyJvMUT17/kECurawGUD1jhVaCZan62C+CCeCiA
WpUIVtLJkuXMm7QslM42hTXobxfZ9V6SibkFEWF7mIyZ3E26hVQSs8WiMUxEoqz6VhBp5+pZ/UIU
yXvqEwhTonPoAYw2FMmJgtW+gIP7U5Wblrz/00kMCjdJV9nqh/v6pbNfoF6juU/6gKXGWZTM2PKXp
w9tAt8E4IxtO135j2OXuCPZ8cUMMuZzQXvfnOrp5cHYqrd9rJWgwTPv6G8lPH6s1YmEVYHkyuavO
Kej4naKjtQOt0phAbnmUS6HS4rjX+h5EUFaHkSG1vfbxovQvcXHQDkP0sE1gEap4Aqf8v14oZo
oB7DA7sDkfq2s9hnvfxDbhO115jhV7UlUw==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - Timestamp 2021*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Tue Apr 13 11:32:20 CEST 2021*

Valid to: *Tue Dec 31 05:02:00 CET 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CD:08:9C:C3:85:94:6D:7F:D1:6D:39:00:46:1E:DF:2B:44:BA:55:56:52:AC:20:B0:08:32:EA:E3:F4:BA:AD:D6:0F:6E
:32:0C:1C:F6:9A:26:7D:AE:C8:83:8B:F5:B9:CC:DE:50:C0:78:7B:AA:5F:FD:E2:AD:3C:85:32:89:C1:8E:9A:EB:44:11:2B:11:C4:9B:1B:C6:6E:F0:26:A0:26:EF:AA:C8:DB:F8:42:C6:39:52:B0:19:AC:D0:CA:E8:23:18:E1:2A
:F7:B7:7A:0E:0D:F7:B9:6E:62:71:12:5A:B4:BD:49:EB:78:77:82:6A:DA:55:C6:A4:48:C2:2F:3C:5F:74:08:3C:26:FB:C7:77:6E:71:5A:92:33:D9:8E:EF:3C:80:B5:D3:C0:E7:40:A0:DC:04:2E:C4:11:75:04:35:BE:23:44:72:2B:7
7:BC:0B:8E:0C:C6:CE:B7:DC:DD:22:33:9B:BC:D7:3C:EB:25:49:16:27:7F:78:0E:86:16:F0:5B:9A:6F:4E:AB:D9:81:C2:7F:4F:04:B4:93:C3:16:DE:A6:5D:77:C2:B3:4F:91:7E:F2:74:10:A8:F3:42:5F:CE:F6:45:96:77:C9:3E:9
E:F2:7F:B5:F8:25:43:D0:98:0E:AC:5A:2D:F4:B9:6A:98:47:B0:54:2F:D0:E5:E8:48:00:4F:1C:D8:29:B1:29:F4:36:66:A1:1E:F6:90:0F:52:60:7B:FE:F4:CE:EB:E9:C5:D4:03:66:29:C1:D6:BD:2F:14:52:EB:3C:CB:07:9D:1B:4F:
C9:CF:B6:8D:45:72:BE:C5:C0:D3:F6:11:2A:95:87:75:36:59:94:F7:5C:24:C8:B8:CC:43:E9:E9:F8:4D:05:B0:3E:A5:FE:EE:C9:16:46:FE:93:53:69:A9:E1:79:36:58:99:95:9F:C2:93:05:29:69:48:EE:BB:42:00:8B:4C:8E:37:88:6
7:01:15:5A:19:01:D4:E0:C4:82:FD:02:6A:D9:10:65:CC:82:FA:62:F7:C3:68:B0:F1:A7:51:8D:91:A1:6A:52:99:9E:AF:C6:1B:83:4A:05:4D:B2:E7:D9:BB:32:21:D9:5E:FB:97:B7:07:6A:B7:A0:B3:8D:35:08:58:23:9C:46:81:B1
:0B:C7:52:9E:E0:81:2B:3E:98:D0:F0:AA:D7:4F:18:F7:10:19:2C:74:4A:21:B0:C3:C5:48:EE:C6:B8:51:E0:D7:BC:B8:DD:F3:F5:63:F0:99:A0:E4:BE:FB:21:91:53:2E:90:78:DE:8F:C4:D5:58:57:7D:B6:CC:99:2F:72:09:88:1C:
D9:23:8B:B0:F6:E7:44:EF:A9:2A:C8:BA:7E:48:91:C1:10:64:46:28:0F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points	*http://crl.firmaprofesional.com/fproot.crl*
Subject Key Identifier	*16:A6:B4:B1:6C:C4:DB:DF:38:47:4C:1A:C0:46:36:58:DE:2C:EB:62*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*75:B1:4D:4D:63:80:6F:30:F5:38:06:0F:2E:B6:5C:13:65:BF:C0:CD:7F:3E:CD:C6:C0:07:02:18:B6:E4:67:59*

X509SubjectName

Subject CN:	*AC Firmaprofesional - Timestamp 2021*
Subject OU:	*Security Services*
Subject 2.5.4.97:	*VATES-A62634068*
Subject O:	*Firmaprofesional S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*Fqa0sWzE2984R0wawEY2WN4s62I=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-09-01T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Firmaprofesional.aspx*
URI	*[es]*	*https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Firmaprofesional.aspx*

18 - TSP: Tesorería General de la Seguridad Social

.

TSP Name

Name	*[en]*	*Tesorería General de la Seguridad Social*
Name	*[es]*	*Tesorería General de la Seguridad Social*

TSP Trade Name

Name	*[en]*	*Gerencia de Informática de la Seguridad Social*
Name	*[es]*	*Gerencia de Informática de la Seguridad Social*
Name	*[en]*	*Tesoreria General de la Seguridad Social*
Name	*[es]*	*Tesoreria General de la Seguridad Social*
Name	*[en]*	*TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*
Name	*[en]*	*VATES-Q2827003A*
Name	*[en]*	*SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*
Name	*[es]*	*SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*
Name	*[en]*	*Seg-social*
Name	*[es]*	*Seg-social*

PostalAddress

Street Address	*[en]*	*Calle Doctor Tolosa Latour*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28041*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Calle Doctor Tolosa Latour*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*

Postal Code	*[es]*	*28041*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:ACGISS.Soporte.giss@seg-social.es*
URI	*[en]*	*http://www.seg-social.es*
URI	*[en]*	*https://sede.seg-social.gob.es*

TSP Information URI

URI	*[en]*	*http://www.seg-social.es/ACGISS*

18.1 - Service (withdrawn): Qualified certificates issued by GISS

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified certificates issued by GISS*
Name	*[es]*	*Certificados reconocidos emitido por GISS*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*1045226008*
X509 Certificate	

-----BEGIN CERTIFICATE-----

MIIC7TCCAlagAwIBAgIEPkziGDANBgkqhkiG9w0BAQUFADAwMQswCQYDVQQGEwJFUzETMBEGA1UE
ChMKU2VyaLXNvY2lhbDEMMAoGA1UECxMDU0dlMB4XDTAzMDIxNDEyMDMyGFoXDTIzMDIxNDEyMzMy
OFowMDELMAkGA1UEBhMCRVMxEzARBgNVBAoTCFNlZy1zb2NpYWwxDDAKBgNVBAsTA1NHSTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEApsifKXmaLgurUtKfmgthAiE184EVGs8gv58GTUv32iVZ
fwf9QRzajfI3haSWlzOv39czeV2dRnoiIVtGgMRFLhaxtEsNitj4ZnYxWHYp59IRR3cgykkPbH8
nk8NZzr8XGo3PPY2Cyp2XSdArrUzPqcBrrSZCsIieFOWzYcz30CAwEAAaOCARIwggEOMBEGCWCG
SAGG+EIBAQQEAwIABzBSBgNVHR8ESzBJMEegRaBDpEwPzELMAkGA1UEBhMCRVMxEzARBgNVBAoT
CFNlZy1zb2NpYWwxDDAKBgNVBAsTA1NHSTENMAsGA1UEAxMEQ1JMMTArBgNVHRAEJDAigA8yMDAz
MDIxNDEyMDMyOFqBDzIwMjMwMjE0MTIzMzI4WjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUcXR3
6Dwip1KGUghdwGVkvPMi02fgwHQYDVR0OBBYEFHF0d+g8IqdSblIIXcBlZLzzNNn4MAwGA1UdEwQF
MAMBAf8wHQYJKoZIhvZ9B0EABBAwDhsIVjYuMDo0LjADAgSQMA0GCSqGSIb3DQEBBQUAA4GBAGND
6tDtKs4RAIucLVixgZhaWWwZ+GIK3BxsBlnO1K7nxqewmJDb+bSUUyn5zrMHlBWzfWXXupx+Z+2D
tbqyX+DyzDdKtOOrqpBJGRxR5B2DkoPolfhDxKY9XalyxD8UMmOI35bCtRYeqo/rXH8CqDwHH0VL
CqL1SNH7sACNXlF8

-----END CERTIFICATE-----

Signature algorithm:	*SHA1withRSA*
Issuer OU:	*SGI*
Issuer O:	*Seg-social*

Issuer C:	*ES*
Subject OU:	*SGI*
Subject O:	*Seg-social*
Subject C:	*ES*
Valid from:	*Fri Feb 14 13:03:28 CET 2003*
Valid to:	*Tue Feb 14 13:33:28 CET 2023*
Public Key:	*30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:A6:C8:9F:29:79:9A:2E:0B:AB:52:D2:9F:9A:07:E1:02:21:35:F3:81:15:1A:CF:20:BF:9F:06:4D:4B:F7:DA:25:59:7F:07:FD:41:1C:DA:8D:FD:77:85:AE:56:97:33:AF:DF:D7:B3:79:5D:9D:46:7A:22:95:5B:62:1A:03:11:14:B8:5A:C6:D1:2C:36:2B:63:E1:99:D8:C5:61:D8:A7:9F:65:45:1D:DC:83:29:24:3E:11:FC:9E:4F:0D:67:3A:FC:5C:6A:37:7C:F6:36:0B:2A:76:5C:94:9D:02:BA:D4:CC:FA:9C:06:BA:D2:64:2B:25:89:E1:4E:5B:36:1C:CF:7D:02:03:01:00:01*
CRL Distribution Points	*C=ES,O=Seg-social,OU=SGI,CN=CRL1*
Authority Key Identifier	*71:74:77:E8:3C:22:A7:52:86:52:08:5D:C0:65:64:BC:F3:34:D9:F8*
Subject Key Identifier	*71:74:77:E8:3C:22:A7:52:86:52:08:5D:C0:65:64:BC:F3:34:D9:F8*
Basic Constraints	*IsCA: true*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F8:00:14:4F:1B:0F:26:83:42:3F:3D:03:3A:4E:5B:B8:A4:67:59:9C:BB:06:36:2C:4C:19:C1:A9:D8:C2:51:B9*

X509SubjectName

Subject OU:	*SGI*
Subject O:	*Seg-social*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-05-03T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

18.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.4.2.1.3*

18.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.1.3 - History instance n.1 - Status: granted

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by GISS*
Name	*[es]*	*Certificados reconocidos emitido por GISS*

Service digital identities

X509SubjectName

Subject OU:	*SGI*
Subject O:	*Seg-social*
Subject C:	*ES*

X509SKI

X509 SK I	*cXR36Dwip1KGUghdwGVkvPM02fg=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

18.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.4.2.1.3*

18.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by GISS*

Name *[es]* *Certificados reconocidos emitido por GISS*

Service digital identities

X509SubjectName

Subject OU: *SGI*

Subject O: *Seg-social*

Subject C: *ES*

X509SKI

X509 SK I *cXR36Dwip1KGUghdwGVkvPM02fg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-04-20T00:00:00Z*

18.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.4.2.1.3*

18.2 - Service (withdrawn): Qualified certificates issued by SUBCA GISS01

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en]	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by SUBCA GISS01*

Name *[es]* *Certificados reconocidos emitido por SUBCA GISS01*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1466067264*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIIxDCCBqygAwIBAgIEV2JpQDANBgkqhkiG9w0BAQsFADCBtjELMAkGA1UEBhMCRVMxDzANBgNV
BAcMBk1BRFJJRDExMC8GA1UECgwoVEVTT1JFUklBIEdFTkVSQUwgREUgTEEgU0VHVVJIREFEIFNP
Q0IBTDE3MDUGA1UECwwuR0VSRU5DSUEgREUgSU5GT1JNQVRJQ0EgREUgTEEgU0VHVVJIREFEIFNP
Q0IBTDESMBAGA1UEBRMJUTI4MjcwMDNfBMRYwFAYDVQQDDA1SQUlaIFJDR0lTU3YyMBkXDTE2MDYx
NjA5NTExN1oXDTMxMDYxNjEwMjExN1owgcYxCzAJBgNVBAYTAkVTMQ8wDQYDVQQHDAZNQURSSUQx
MTAvBgNVBAoMKFRFU09SRVIJQSBHRUSFUkFMIERFIExBIFNFR1VSSURBRCBTT0NJQUwxNzA1BgNV
BAsMLkdFUkVOQ0IBIERFIEIORk9STUFUSUNBIERFIExBIFNFR1VSSURBRCBTT0NJQUwxDzANBgNV
BAsMBkdU1MwMTESMBAGA1UEBRMJUTI4MjcwMDNBMRUwEwYDVQQDDAxTVUJDQSBHSVNTMDEwggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCmoxDF3OPJ6tZDRzx9FzluK+U9UwfAV2V+0DzG
lZC9ZvZHf0nDg+OTxOn+f7EJGtCJX2FGBC0Jua/0AB87vAeAlAvPJ2GC6EU8IAnGsYhuJsmBNDHY
zscPhI2CBoyXa3otsnfOB0vdGVPVZnKRLybPjchwHIrnBP90+ejpUdJ1wDu8jDYCzVFWKmPFmz
LK2n4oMqcYDjhealqwerx4ArNtFYi5ioZGk2cvHUzCSTvrwale9ZCiHntAp/nqdR5KLHzTiK4HLZ
VPOAgEVY8obv98Tjpl/RRVsa9JWNbY8GImRCcs7bTSOrMR5TL3/7aevLKLAPH7+On1D2zpnL Nur
bqotHbktBKlzobOZv/vta1UuzilkOD+hCsSvuz2ocQWC6BPZVSJL3akZCM1/2+lw7xyUuHbgD7Fk
xiT5zsS7Pcud6coUvwKJ7U7bwCx+wqEG3PAC4liWfRKBjy9JOWQsp/M8uuoWtPef3d4tSVWyC+4S
hEDQreADRte3rO8bMqVjgbpIL+tIfxFZVlbPbbqlbcSccrksRLIqIEC14iD3/BMu86053JYp5Im
pb1roJVSXyC0PsafjIFiAtiIKqBCukLfAktrhpWqlOta G6D+xk6Kv8Ertfz92uwRVz+W9cZszACXVG
j5tG66YK8r/49ymth6mea5OwdT9mxFl9hHn20wIDAQABo4ICxjCCAsIwDgYDVR0PAQH/BAQDAgEG
MA8GA1UdEwEB/wQFMAMBAf8wgc8GA1UdIASBxzCBxDCBwQYIYIVUAQQCAgEwgbQwKwYIKwYBBQUH
AgEWH2h0dHA6Ly93d3cuc2VnLXNvY2lhbC5lcy9BQ0dU1MwgYQGCCsGAQUFBwICMHgadkNlcnRp
ZmlyYWRvIGRlIGxhIENBIFNYYm9yZiluYWRhIEdU1MwMSBkZSBBQ0dU1N2Md5Db25zdWxlZSBs
YXMgY29uZGljaW9uZXMgZGUgdXNvIGVuIGh0dHA6Ly93d3cuc2VnLXNvY2lhbC5lcy9BQ0dU1Mw
fAYIKwYBBQUHAQEEcDBuMCoGCCsGAQUFBzABhh5odHRwOi8vb2Nzcc5zZWctc29jaWFsLmdvYi5l
cy8wQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuc2VnLXNvY2lhbC5lcy9BQ0dU1MvQ2VsdHMvUkFJ
W9BQ0dU1NfVjIwggENBgNVHR8EggEMMIIBADAqoCigIoYkaHRtcDovL2NybC5zZWctc29jaWFs
LmdvYi5lcy9hcmwuY3JsMIHRoIHOoIHLplHIMIHFMQswCQYDVQQGEwJFUzEPMA0GA1UEBwwGTUFE
UklEMTEwLwYDVQQKDChURVNPUkVSSUEgR0VORVJBTCBERSBMQSBTRUdlVUklEQUQgU09DSUFMMTcw
NQYDVQQLDC5HRVJFTkNJQSBERSBJTkZPUk1BVEIDQSBERSBMQSBTRUdlVUklEQUQgU09DSUFMMRIw
EAYDVQQFEwlRMjgyNzAwM0IEoFjAUBgNVBAMMDVJBSVoqQUNHSVNTdloDTALBgNVBAMMBENSTDEw
HwYDVR0jBBgwFoAU43jTkFYoHtLvLBTkY5t00c75k0wHQYDVR0OBBYEFI1KI1tvkjkHGhfZeYCq
1hoaf/bTMA0GCSqGSIb3DQEBCwUAA4ICAQCfyT1+caPGAxr17U1WOmWoKZhDMxAn2ORrhpYhml+K
5ABV9XzBIY4FDc1af4N4d37nM78GVe05vH3gmENVb4sU/b+Ek2d6nH1LpC3bT8RbLCZRw9Vx2tq3K
U/wKBDvrP/7BwORmcwsmURApLL3dIoJC2FAWaODpeNt06ByQ++ahwcyW6fvVgsIQZ+Cq5qOeYaXyA
9XeTDrjxOhAny2RFhmBRWFt5iHKY+0TSIPzlohIOzQ4cDk1zs4rNmngdLsFYW4EiT5Ep2wPr7D9P
jQMZISW1d7a/GUnqr56dnWMR3nczkMar04e4Gtj+JjOYh+apb7OdHGVa+vLgB0VA/w7pT/KPR0/1
8nUoCrqQATsjziBjQyIBHKesNgNrkLXBEWY/AIfndZ3BxboB2+c8twNk7ndYDN67RtYI2ORk6ndf
GP9PCrODn9EHOP+d6Nms+PISPBsxC1JMWrgiM7nKA9ma5AHhi+gIDlkh+AAb0I9L8zt+n0IZHI+B
XBVBurGycTx5WacbMGIFxZQANTo1tq9lZBqOtOei3eLHVQE7MyHz1yNMr+zBwfvpgbRRJWCiq
G4afIvyNrgXohcBYxySQx3DduCnjqi6uAy/hDXWhJukODJtRj52chSscxRVW6o84UOmHg04C6kCb
5pcpouijkTcaY+vPNETVMjuON5F8bBb2zw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *RAIZ ACGISSv2*

Issuer SERIAL NUMBER:	*Q2827003A*
Issuer OU:	*GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*
Issuer O:	*TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*
Issuer L:	*MADRID*
Issuer C:	*ES*
Subject CN:	*SUBCA GISS01*
Subject SERIAL NUMBER:	*Q2827003A*
Subject OU:	*GISS01*
Subject OU:	*GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*
Subject O:	*TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*
Subject L:	*MADRID*
Subject C:	*ES*
Valid from:	*Thu Jun 16 11:51:17 CEST 2016*
Valid to:	*Mon Jun 16 12:21:17 CEST 2031*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:A3:10:C5:DC:E3:C9:EA:D6:43:47:3C:7D:17:32:2E:2B:E5:3D:53:07:C0:57:65:7E:D0:3C:C6:95:90:BD:66:F6:47:7F:49:C3:83:E3:93:C4:E9:FE:7F:B1:09:1A:D0:89:5F:61:46:04:2D:09:B9:AF:F4:00:1F:3B:BC:07:80:94:0B:CF:27:61:82:E8:45:3C:20:09:C6:B1:88:6E:26:C9:81:34:31:D8:CE:C7:8F:85:FD:82:06:8C:97:6B:7A:2D:B2:77:CE:07:4B:E2:74:65:4F:55:99:CA:44:BC:9B:3E:37:21:C0:72:2B:88:13:FD:D3:E7:A3:A5:47:48:DF:5C:03:BB:C8:C3:60:2C:D5:15:62:A6:3C:59:B3:2C:AD:A7:E2:83:2A:71:80:E3:85:E6:A5:AB:07:AB:C7:80:2B:36:D1:58:8B:98:A8:64:69:36:72:F1:D4:CC:24:93:BE:BC:1A:21:EF:59:0A:21:E7:B4:0A:7F:8A:A7:51:E4:A2:C7:CD:3B:4A:E0:72:D9:56:5F:4E:02:0E:95:63:CA:21:BF:DF:35:A6:5F:D1:45:5B:1A:F4:95:8D:6D:8E:6D:18:89:91:09:EE:7B:85:34:8E:AC:C4:79:4C:BD:FF:ED:A7:AF:2C:A2:C0:3C:7E:FE:3A:74:F4:DB:2C:E9:2C:DB:AB:6E:AA:2D:1D:B9:2D:04:A2:33:A1:B3:99:BF:FB:ED:6B:55:2E:CE:29:64:38:3F:A1:0A:C4:AF:BB:3D:A8:71:05:82:E8:13:D9:55:22:4B:DD:A9:19:08:CD:7F:DB:E9:70:EF:1C:94:B8:76:E0:0F:B1:64:C6:24:F9:CE:C4:BB:3D:CB:9D:E9:CA:14:BF:02:A5:ED:4E:DB:C0:2C:7E:C2:A1:06:DC:F0:02:E2:58:96:7D:12:81:8F:2F:49:39:64:2C:A7:F3:3C:BA:EA:16:B4:F7:9F:DD:DE:2D:49:55:B2:0B:EE:12:84:40:D0:AD:E0:03:46:D7:B7:AC:E6:CC:A9:58:E0:6E:99:4B:F9:F2:1F:C4:56:55:95:B3:DB:6E:A9:5B:71:27:9C:AE:4B:11:23:F2:2A:7C:40:88:E2:20:F7:FC:13:2E:F3:AD:39:DC:96:29:E5:F9:66:A5:BD:6B:A0:95:52:5F:20:B4:3E:CB:1F:8F:51:62:02:D8:B5:2A:A0:42:BA:42:DF:02:4A:E1:A5:6A:A5:39:A1:BA:0F:EC:7C:E8:AB:FC:12:BA:DF:CF:DD:AE:C1:15:73:F9:6F:5C:66:CC:C0:09:75:46:8F:9B:46:EB:A6:0A:F2:BF:F8:F7:29:AD:87:A9:9E:6B:93:B0:75:3F:66:C4:59:7D:84:79:F6:D3:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Certificate Policies	*Policy OID: 2.16.724.1.4.2.2.1* *CPS pointer: http://www.seg-social.es/ACGISS* *CPS text: [Certificado de la CA Subordinada GISS01 de ACGISSv2.Consulte las condiciones de uso en http://www.seg-social.es/ACGISS]*
Authority Info Access	*http://ocsp.seg-social.gob.es/* *http://www.seg-social.es/ACGISS/Certs/RAIZ_ACGISS_V2*
CRL Distribution Points	*http://crl.seg-social.gob.es/arl.crl* *C=ES,L=MADRID,O=TESORERIA GENERAL DE LA SEGURIDAD SOCIAL,OU=GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL,SERIALNUMBER=Q2827003A,CN=RAIZ ACGISSv2,CN=CRL1*
Authority Key Identifier	*E3:78:D3:90:56:28:1E:D2:EF:2C:14:E4:62:5E:62:D3:47:3B:E6:4D*
Subject Key Identifier	*8D:4A:D5:FD:72:92:3F:07:1A:11:5F:CD:80:AA:D6:1A:1A:7F:F6:D3*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A9:20:D6:61:E8:D9:0D:A3:07:AB:B1:1C:AC:5E:00:FF:93:02:26:AE:B0:FE:B6:A8:81:49:C6:55:95:5B:03:E1*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-10-26T01:00:00Z*

18.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

18.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.4.2.2.1.1.2*

Description

18.2.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by SUBCA GISS01*

Name [es] *Certificados reconocidos emitido por SUBCA GISS01*

Service digital identities

X509SubjectName

Subject CN: *SUBCA GISS01*

Subject SERIAL NUMBER: *Q2827003A*

Subject OU: *GISS01*

Subject OU: *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

Subject O: *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-05-03T00:00:00Z*

18.2.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

18.2.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.1.4.2.2.1.1.2

Description

18.2.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by SUBCA GISS01*

Name [es] *Certificados reconocidos emitido por SUBCA GISS01*

Service digital identities

X509SubjectName

Subject CN: *SUBCA GISS01*

Subject SERIAL NUMBER: *Q2827003A*

Subject OU: *GISS01*

Subject OU: *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

Subject O: *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

18.2.5.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.4.2.2.1.1.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.1.4.2.2.1.1.1*

18.2.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.2.6 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified certificates issued by SUBCA GISS01*
Name	*[es]*	*Certificados reconocidos emitido por SUBCA GISS01*

Service digital identities

X509SubjectName

Subject CN:	*SUBCA GISS01*
Subject SERIAL NUMBER:	*Q2827003A*
Subject OU:	*GISS01*
Subject OU:	*GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*
Subject O:	*TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-23T22:00:00Z*

18.2.6.6 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.4.2.2.1.1.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.1.4.2.2.1.1.1*

18.3 - Service (withdrawn): Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*

Name *[es]* *Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1466133214*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHgzCCBWugAwIBAgIEV2Nq3jANBgkqhkiG9w0BAQsFADCBxjELMAkGA1UEBhMCRVMxDzANBgNV
BAcMBk1BREFJRDEsMCIGA1UECgwsVEVTVFJ1JkIlIEdfTk VSQUwgREI1g7EEgU0VHVVJIREFEIFNP
Q0lBTDE3MDUGA1UECwwuR0VSRU5DSUEgREUgSU5GT1JNQVRJQ0EgREUgTEEgU0VHVVJIREFEIFNP
Q0lBTDEPMA0GA1UECwwGR0lTUzAxMRIwEAYDVQQFEwlRMjgyNzAwM0ExFTATBgNVBAMMDFNVQkNB
IEdJU1MwMTAeFw0xNjExMjQxMjIyMTFaFw0yMTExMjQxMjIyMTFaMIG7MQswCQYDVQQGEwJFUzE0
MDIGA1UECgwrU0VDUkVUQVJJQSBERSBFU1RBRE8gRE1gTEEgU0VHVVJIREFEIFNP0lBTDEfMB0G
A1UECwwWU0VSVkIDSU9TIERFIENPTkZJQU5aQTFYMBAGA1UEBRMJUzI4MTkwMDFFMBYGA1UEYQwP
VkFURVMtUzI4MTkwMDFFMCKGA1UEAwwiVFNBIEFVVE9SSURBRCBERSBTRUxMQURPIERFIFRJRU1Q
TzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMnzqjCMnsU445zh8ea7UNd07OPDbjcI
jqssX/++UScQWGP8IQWRL6CuMShjkWPxtbSL/1aF/2ceZPG4z6bXDsMn1donCNF6Kut0u8ismDp5
522/Gtxuxy0OqdfR/Qzxuyr2U/BBec+NTHOekPNJBCkKCBXxPYWZucb64AajNQemyhzWt6NpgE704
AmkBvEJbL16n6IVGV07K3159nymXYxAb91CIYjTeDsul5oBRcl/GdzdOIGlPccMBRuIVIp1YF2x
jKZ8lcm2hp9zP3KySuWlszDOiJGUNiPoC9QkFkwaA7BizXKBO92uuaIDEkv7aV7Xr8QbzpPzxc4/
7+qbEnCAwEAaOCAoAwggJ8MA4GA1UdDwEB/wQEAwIGwDAWBgNVHSUBAI8EDDAKBggrBgEFBQcD
CDB0BggrBgEFBQcBAQRoMGYwKgYIKwYBBQUHMAGGHmhtdHA6Ly9vY3NwLnNlZy1zb2NpYWwuZ29i
LmVzLzA4BggrBgEFBQcwAoYsaHR0cDovL3d3dy5zZWctc29jaWFsLmVzL0FDR0ITUy9TVUJDQV9H
SVNTMDEwWwYIKwYBBQUHAQMETzBNMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wCQYHBACORgEGAjAp
BgYEAI5GAQUWH2h0dHA6Ly93d3cuc2VnL.XNvY2lhbC5lcy9BQ0dUU1MwgcAGA1UdIASBuDCBrTCB
sgYKYIVUAQQCAgEDATCBozAzBggrBgEFBQcCARYfaHR0cDovL3d3dy5zZWctc29jaWFsLmVzL0FD
R0ITUzB0BggrBgEFBQcCAjBoGmZDZXJ0aWZpY2FkbyBkZSBzZWxsYWRvIGRlIHRpZW1wby4gQ29u
c3VsdGUgbGFzIGNvbmRpY2lvbmVzIGRlIHVzbyBlbiBodHRwOi8vd3d3LnNlZy1zb2NpYWwuZXMv
QUNHSVNTDQowNwYDVR0SBDAwLoEscmZjODIyTmFtZT1hY2dpc3Muc29wb3J0ZS5naXNzQHNlZy1z
b2NpYWwuZXMwOAYDVR0BDEwLAAtsCigKYYnaHR0cDovL2NybC5zZWctc29jaWFsLmdvYi5lcy9h
Y19zdWluY3JsMB8GA1UdIwQYMBaAFIKIYykzHGhfGYCq1hoaf/bTMB0GA1UdDgQWBBSqJoeU
BBKDgFpvcITOU65xOxu8XzAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4ICAQAVhZJJzme8nQqe
y9ZApuA2ZsvlQFSqEqC8I5gyDfXdM25njm7EaGMzn6cfmu3S+aKVA5zwU45tHkPxFRmZYoWZWxt
Lk325e9ams7BEz+nAq/ft38ih2ePFgkC6RPbGDxIcDlNYpvfD02Gcv2vRcWSCFC6wg7ZrLnBIzp
j4yFxyrzk3G8GBMTKmZWSiDpuJ4EtS6aSuV9DY5cXl/AUw949J4b4Fx58kDTwmb7SaWIrk7B5iR6
R162ic6xxPE7xUGYdakbDARfA32jx29zDtIZ18549gGNlLUylq+y8PK8s1xbXmRHRmixTxcmt+Gl
wqy0cELEKrc74YIYjzuZSPqjG9KcPQpKbaFgW3FGGX/JQY2TG04laoy4Kw9GvXIzDneegGPqQSE0
6r7i97nstb+WFkJBSJ5ADVcwa6MeYmmcWjfgDc4k00UpwaEi6pbB7ycdik7RDm4jlhDqwDkJ5JI0
OZpcp4pDdtJDahCxdsXK0U/YIxTPpwBA8HvfiuqOOrgsMRaUb1Ib+NEnFcOWCK6fdab/9s2M3kNWHj
PfS4uPHZdGcG67hW2FElzd23FkiZF4UAFvFX1XqRlFSSOMGv6fXcFzfc12Oumun89Du9EQ7CfIxD
zeeqkILmUT4RzLxYb+97GLlWFGwX8foWuvxQrMq/JLFlhNR2ZdRAmXxSAThxqQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *SUBCA GISS01*

Issuer SERIAL NUMBER: *Q2827003A*

Issuer OU: *GISS01*

Issuer OU: *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

Issuer O: *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

Issuer L: *MADRID*

Issuer C: *ES*

Subject SERIAL NUMBER: *S2819001E+2.5.4.97*

Subject OU: *SERVICIOS DE CONFIANZA*

Subject O: *SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*

Subject C: *ES*

Valid from: *Thu Nov 24 13:22:11 CET 2016*

Valid to: *Wed Nov 24 13:52:11 CET 2021*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C9:F3:AA:30:8C:9E:C5:38:E3:9C:E1:F1:E6:BB:50:D7:74:EC:E3:C3:6E:37:08:8E:AB:2C:5F:FF:BE:51:27:10:58:63:F
C:21:05:91:2F:A0:AE:31:28:63:91:63:F1:B5:B4:8B:FF:56:85:FF:67:1E:64:F1:B8:CF:A6:D7:0E:C3:27:D5:DA:27:08:D1:7A:2A:EB:74:BB:C7:EC:98:3A:79:E7:6D:BF:1A:DC:6E:C7:2D:0E:81:D1:51:8D:0C:F1:BB:26:54:04:
17:9C:F8:D4:C7:39:E9:0F:34:90:42:B0:AF:C2:05:7C:4F:61:66:6E:73:4E:B8:01:A8:CD:41:E9:F2:87:35:A2:E8:DA:60:13:BD:38:02:69:01:BC:42:5B:2E:5E:A7:EA:55:46:57:4E:CA:DE:5E:7D:9F:29:9F:5D:8C:40:6F:DD:42:7
D:88:D3:78:3B:2E:97:9A:01:45:E9:7F:19:DC:DD:38:81:A5:3D:C7:0C:05:1B:88:54:8A:75:60:5D:B1:8C:A6:7C:95:C9:B6:86:9F:73:3F:72:B2:4A:E5:A5:B3:30:CE:88:91:94:36:23:E8:0B:D4:24:16:4C:1A:03:B0:62:CD:72:81:
3B:DD:AE:B9:A2:03:12:4B:FB:69:5E:D7:AF:C4:1B:CE:93:F3:C5:CE:3F:EF:EA:9B:12:B7:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Authority Info Access

http://ocsp.seg-social.gob.es/

http://www.seg-social.es/ACGISS/SUBCA_GISS01

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

Certificate Policies	*Policy OID: 2.16.724.1.4.2.2.1.3.1* *CPS pointer: http://www.seg-social.es/ACGISS* *CPS text: [Certificado de sellado de tiempo. Consulte las condiciones de uso en http://www.seg-social.es/ACGISS]*
Issuer Alternative Name	*rfc822Name=acgiss.soporte.giss@seg-social.es*
CRL Distribution Points	*http://crl.seg-social.gob.es/ac_sub.crl*
Authority Key Identifier	*8D:4A:D5:FD:72:92:3F:07:1A:11:5F:CD:80:AA:D6:1A:1A:7F:F6:D3*
Subject Key Identifier	*AA:26:8A:14:04:12:83:80:5A:6F:72:54:CE:53:AE:71:3B:1B:BC:5F*
Basic Constraints	*IsCA: false*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*EB:A2:BD:4B:A5:BD:CA:E7:73:A4:BA:EF:9E:59:74:83:AA:97:20:C2:5D:7C:AF:C7:4A:22:C4:DA:9A:76:02:09*

X509SubjectName

Subject SERIAL NUMBER:	*S2819001E+2.5.4.97*
Subject OU:	*SERVICIOS DE CONFIANZA*
Subject O:	*SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*
Subject C:	*ES*

X509SKI

X509 SK I	*qiaKFAQSg4Bab3JUzlOucTsbvF8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-10-26T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

18.3.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name	*[en]*	*Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*
Name	*[es]*	*Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*

Service digital identities

X509SubjectName

Subject SERIAL NUMBER:	*S2819001E+2.5.4.97*
Subject OU:	*SERVICIOS DE CONFIANZA*
Subject O:	*SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*
Subject C:	*ES*

X509SKI

X509 SK I	*qiaKFAQSg4Bab3JUzlOucTsbvF8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-05-03T00:00:00Z*

19 - TSP: Ministerio de Empleo y Seguridad Social

.

TSP Name

Name	*[en]*	*Ministerio de Empleo y Seguridad Social*
Name	*[es]*	*Ministerio de Empleo y Seguridad Social*

TSP Trade Name

Name	*[en]*	*Ministerio de Empleo y Seguridad Social*
Name	*[es]*	*Ministerio de Empleo y Seguridad Social*
Name	*[en]*	*Ministerio de Trabajo e Inmigracion*
Name	*[es]*	*Ministerio de Trabajo e Inmigracion*
Name	*[en]*	*VATES-S2819001E*
Name	*[en]*	*MINISTERIO DE TRABAJO E INMIGRACION*
Name	*[en]*	*MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*

PostalAddress

Street Address	*[en]*	*Paseo de la Castellana, 63*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28071*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Paseo de la Castellana, 63*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28071*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:admin_ca@meyss.es*
URI	*[en]*	*http://www.meyss.es*

TSP Information URI

URI	*[en]*	*https://ca.empleo.gob.es/en/CA_MEYSS/index.htm*
URI	*[es]*	*https://ca.empleo.gob.es*

19.1 - Service (withdrawn): Certificados Reconocidos emitidos por la AC1 RAIZ MTIN

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por la AC1 RAIZ MTIN*
Name	*[en]*	*Qualified Certificates issued by AC1 RAIZ MTIN*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1304969050763335590*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJTTCCBzWgAwIBAgIIEhwucAmgl6YwDQYJKoZIhvcNAQELBQAwgeIxFjAUBgNVBAMTDUFDMSBS
QUlaIE1USU4xEjAQBgNVBAUTCVMyODE5MDAxRTE1MDMGA1UECxMsUFJFU1RBRE9SIERFIFNFUZJ
Q0lPUyBERSBDRVJUSUZJQ0lFDSU9OIE1USU4xMTAvBgNVBAsTKFNVQkRJUkVDQ0lPTyBHRU5FUkFM
IERFIFBST0NFU08gREUgREFUT1MxLDAqBgNVBAoTI01JTkITVEVSSU8gREUgVFJBQkFKTyBFIEIO
TUlHUkFDSU9OMQ8wDQYDVQQHEwZNQURSSUQxCzAJBgNVBAYTAkVTMB4XDTA5MTEwNTE2MTc0NVoX
DTE5MTEwMzE2MTc0NVowgeIxFjAUBgNVBAMTDUFDMSBSQUlaIE1USU4xEjAQBgNVBAUTCVMyODE5
MDAxRTE1MDMGA1UECxMsUFJFU1RBRE9SIERFIFNFUZJQ0lPUyBERSBDRVJUSUZJQ0lFDSU9OIE1U
SU4xMTAvBgNVBAsTKFNVQkRJUkVDQ0lPTyBHRU5FUkFM IERFIFBST0NFU08gREUgREFUT1MxLDAq
BgNVBAoTI01JTkITVEVSSU8gREUgVFJBQkFKTyBFIEIOTUlHUkFDSU9OMQ8wDQYDVQQHEwZNQURS
SUQxCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA3M3Nsb/eJIX/
HDNzmTwboW31oMR9mzhmjQmtA2xXNbQTQf7jX+YiBFgYuU/5pMwQ/kcfZTv8zNKcyQDKTV/6BryVD
XB39e1eLYgbnZK04+VYIYDmqozIQQkdPEtGEpSSarTXybq1thMYEGamSUTSf8Sx7R1UPt17F9vb/
tHBV9gtZt3QB4POetXzkBIgIUFl4HxqU2+IyYnTN7jzPYbRGcuDWbAHCE+ZdAIH8DIRyPvm0Dwm
dn1yfqx2N8GKdSBcQNyEP9BJfE1nrjnv5M6A4cqd5i2rLuYSldr5+9/j4ow9h/tFbKSr9niSJxSh
XWtPcHtXc+/5XagPdZ/vEWAZhLBkQO7YqYb6pddF9BFv8YbINFuISM663c2b3YjpATborGroEguw
4HuQHoU/LSYkB9v+C31hIfoNI1gfQHGb6ZigtxMP9+JlI1IYK2vxbwIEbHXQpONoU2Fy7Yvqb0s
9T20FzcaUzMedKkG8hzBjR0tPFqyikoxzSEWyPYugCMzAnBx29dBKu3TyZ3qTXPlNqz/zFp0DT7
Jexolgqi3YMfyjyPdDYIVO/1GHvCJDHR+4lErgSC1vUCKXHhknF0jtuqcR3EO8ZiJmyGPCNV6ynR
H6vKHmPnx3O0p7gqOvYf+4dliPzzm/6/69UdtqgD6WWDGYzgGO0X2BwNPZyKWH8CAwEAAaOCAwMw
ggLMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQrQxizxEsclyx/5
8E7830rkFWDIgzA3BggrBgEFBQcBAQQfMCkwJwYIKwYBBQUHMAGGG2h0dHA6Ly9jYS5tdGluLmVz
L210aW4vb2NzcDByBgNVHR8EazBpMDKgMKAuhixodHRwOi8vY2EubXRpbi5lcy9tdGluL2NybC9N
VElOQXV0b3JpZGFkUmFpejAzoDGgL4YtaHR0cDovL2NhMi5tdGluLmVzL210aW4vY3JsL01USU5B
dXRvcmlkYWRSYWl6MIG5BgNVHSAEgbEwgawgasGCysGAQQBgdkFAgQBMIGbMDAGCCsGAQUFBwIB
FiRodHRwOi8vY2EubXRpbi5lcy9tdGluL0lRQQ3IQb2xpdGljYXMwZwYIKwYBBQUHAgIwWxpZQ2Vy
dGlmaWNhZG8gcmHteiAgQ29uc3VsdGUgbGFzIGNvbmRpY2lvbmRpY2lvbmVzIGRlIHVzbyBlbiBodHRwOi8v
Y2EubXRpbi5lcy9tdGluL0RQQ3IQb2xpdGlj YXMwggEYBgNVHSMEggEPMIIBC4AUM0MYs8RLHcsf
+fBO/N9K5BVgyIOhgeikgeUwgeIxFjAUBgNVBAMMDUFDMSBSQUlaIE1USU4xEjAQBgNVBAUTCVMy
ODE5MDAxRTE1MDMGA1UECwwsUFJFU1RBRE9SIERFIFNFUZJQ0lPUyBERSBDRVJUSUZJQ0lFDSU9O
IE1USU4xMTAvBgNVBAsMKFNVQkRJUkVDQ0lPTiBHRUSFUkFMIERFIFBST0NFU08gREUgREFUT1Mx
LDAqBgNVBAoMI01JTkITVEVSSU8gREUgVFJBQkFKTyBFIEIOTUlHUkFDSU9OMQ8wDQYDVQQHDAZN
QURSSUQxCzAJBgNVBAYTAkVTgggSHC5wCaCXpjAbBgNVHRIEFDASgRBhZG1pb19jYUBtdGluLmVz
MBsGA1UdEQQUMBKBEGFkbWluX2NhQG10aWduZXMwDQYJKoZIhvcNAQELBQADggIBAGd0il7Ml0Qh
ZJSacRgRPAZETEivIH2+QSPJrJcGEgH5+SKbIH/ihfPLVJmW+sP+RDNd+cGpMRrPi7jqIe9SGTVm
+uDCIGk4Gpcj+u0YMrRhSvtZ4kpcFKYqQ7xPG4Kkltx8lu5ZJbQLM8CHyp7XQ0tTtFH36YYLooi
db4Tb+PTzrPzD0Aayoax9ZiG2V8bwI3TaGpLIbILK8DbXgGAD0YQjcRySBoz4H8P8WjK54RMnjZ3
zCrxo11QvgfQUiSGcsCNobzGYw/6uWq6wcugEqNjApy7nO4uLyOtyGQ9Ctr3n3zZd0Ndb75NI+Iy
j91KUqU1y6UaF3LHZ0CgzGElsT2WO2tgS8wlUUk2Yv6T+qI0pOZ8ZRHdcE5tbg4BxySc+2pvaIB
dObQcL1SwdDsNTQVdwkIFc3VkaS58+ekNziBglRdnezrtElxl+msruqxH3EOSvpWds5t0pj0WC3el
Bb0tHakSLQVAEyMgX1I+ZDj6dkJPg9u3Bach4Vz7hIRhdBHbr7HWRdKDZ/s8DAOJTEL d5czoQdP
TQVUWtrK+149mHtGCIngZj4Om0Sc25BEiihap4vRy5JGUXzhty6O4mnXcr6AuRnWLBT2JPyCOJJ9a
HWEKnnD2jyMKmGac0gqXcHIxDc4zu6XL7HhA9AFBwFuDmSZefxA7WmxK643qsk7n

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L:	*MADRID*
Issuer O:	*MINISTERIO DE TRABAJO E INMIGRACION*
Issuer OU:	*SUBDIRECCION GENERAL DE PROCESO DE DATOS*
Issuer OU:	*PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*
Issuer SERIAL NUMBER:	*S2819001E*
Issuer CN:	*AC1 RAIZ MTIN*
Subject C:	*ES*
Subject L:	*MADRID*
Subject O:	*MINISTERIO DE TRABAJO E INMIGRACION*
Subject OU:	*SUBDIRECCION GENERAL DE PROCESO DE DATOS*
Subject OU:	*PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*
Subject SERIAL NUMBER:	*S2819001E*
Subject CN:	*AC1 RAIZ MTIN*
Valid from:	*Thu Nov 05 17:17:45 CET 2009*
Valid to:	*Sun Nov 03 17:17:45 CET 2019*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DC:CD:CD:B1:BF:DE:25:F5:FF:1C:33:73:99:3C:1B:A1:6D:F5:A0:C4:7D:9B:38:66:8D:09:DF:03:6C:57:35:B4:13:41:FE:E3:5F:E6:22:04:58:18:B9:4E:69:33:04:3F:95:C7:D9:4E:FF:33:34:A7:32:40:32:93:57:FE:81:AF:25:43:5C:1D:FD:7B:57:0B:62:08:67:67:62:B4:E3:E5:58:25:80:E6:AA:86:62:40:E7:4F:10:61:29:49:26:AB:4D:7C:A1:AB:5B:61:31:81:06:6A:64:94:4D:27:F8:4B:1E:D1:D5:43:E2:D7:B1:6D:F6:F6:FF:B4:70:55:F6:08:99:B7:74:01:E0:F3:9E:B5:7C:E4:04:88:08:50:59:78:1F:1A:94:DB:EF:C8:C9:89:D3:37:B8:F3:3D:86:D1:19:CB:83:5A:10:07:08:4F:99:74:02:07:F0:32:51:C8:FB:E6:D0:3C:26:76:7D:72:7E:AC:76:37:C1:8A:75:20:5C:40:DC:84:3F:D0:49:7C:4D:67:AE:39:EF:E4:CE:80:E1:CA:9D:E6:2D:AB:2E:E6:12:95:DA:F9:FB:DF:E3:E2:8C:3D:87:FB:45:6E:44:AB:F6:78:92:27:14:A1:5D:6B:4F:70:7B:57:73:EF:F9:5D:A8:0F:75:9F:EF:11:60:19:84:B0:64:40:EE:D8:A9:86:FA:A5:D7:45:F4:11:6F:F1:86:C8:34:5B:88:48:CE:BA:DD:CD:9B:DD:88:E3:01:36:E8:AC:6A:E8:12:0B:B0:E0:7B:90:1E:85:0B:49:89:01:F6:FF:82:DF:58:65:22:83:48:D6:07:D0:1C:66:FC:66:28:3A:C4:C3:E5:F8:99:65:27:52:58:F3:6B:F1:6F:02:44:84:75:D0:A4:E3:68:53:61:72:EF:F6:2F:A9:B3:AC:F5:F4:F6:D0:5C:DC:69:4C:CC:79:D2:A4:1B:C8:73:06:34:74:B4:F1:6A:CA:29:28:C7:34:84:5B:23:D8:BA:00:8C:CC:09:C1:C7:6F:5D:04:AB:B7:4F:26:77:A9:35:CF:20:D6:B3:FF:31:69:D0:34:FB:25:EC:68:96:0A:A2:DD:83:1F:CA:3C:8F:74:36:25:54:EF:F5:18:7B:C2:24:31:D1:FB:82:04:AE:04:82:D6:F5:02:29:71:E1:92:71:74:8E:DB:AA:71:1D:C4:3B:C6:62:26:6C:86:3C:23:55:EB:29:D1:1F:AB:CA:1E:63:E7:B3:73:B4:A7:B8:2A:3A:F6:1F:FB:87:65:88:FC:F3:9F:FE:BF:EB:D5:1D:B6:A8:03:E9:65:83:19:8C:E0:18:ED:17:D8:1C:0D:3D:9C:8A:58:7F:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83*
Authority Info Access	*http://ca.mtin.es/mtin/ocsp*
CRL Distribution Points	*http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz* *http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.27781.2.4.1* *CPS pointer: http://ca.mtin.es/mtin/DPCyPoliticas* *CPS text: [Certificado raíz. Consulte las condiciones de uso en http://ca.mtin.es/mtin/DPCyPoliticas]*
Authority Key Identifier	*33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83*
Issuer Alternative Name	*admin_ca@mtin.es*

Subject Alternative Name *admin_ca@mtin.es*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AC:30:43:35:14:59:BB:46:A3:63:BD:24:A6:9F:56:45:F5:35:B8:09:53:F1:8D:7A:58:50:FB:8E:39:58:3E:C2*

Certificate fields details

Version: *3*

Serial Number: *5545899491963*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJSTCCBzGgAwIBAgIGBQtBXoJ7MA0GCSqGSIb3DQEBBQUAMIHiMRYwFAYDVQQDEw1BQzEgUkFJ
WiBNVEIOMRIwEAYDVQQFEwITMjgxOTAwMUUxNTAzBgNVBAsTLFBSRVNUQURPUiBERSBTRVJWSUNJ
T1MgREUgQ0VSVEIGSUNBQ0lPTiBNVEIOMTEwLwYDVQQLEyhTVUJESVJFQ0NJT04gR0VORVJBTCBE
RSBQUk9DRVNPIERFIERBVE9TMSwwKgYDVQQKEyNNSU5JU1RFUkIPIERFIFRSQUJBSk8gRSBJTk1J
R1JBQ0lPTjEPMA0GA1UEBxMGTUFEUkIEMQswCQYDVQQGEwJFUzAcFw0wOTExMDUxNjE3NDVaFw0x
OTExMDMxNjE3NDVaMIHiMRYwFAYDVQQDEw1BQzEgUkFJWiBNVEIOMRIwEAYDVQQFEwITMjgxOTAw
MUUxNTAzBgNVBAsTLFBSRVNUQURPUiBERSBTRVJWSUNJT1MgREUgQ0VSVEIGSUNBQ0lPTiBNVEIO
MTEwLwYDVQQLEyhTVUJESVJFQ0NJT04gR0VORVJBTCBERSBQUk9DRVNPIERFIERBVE9TMSwwKgYD
VQQKEyNNSU5JU1RFUkIPIERFIFRSQUJBSk8gRSBJTk1JR1JBQ0lPTjEPMA0GA1UEBxMGTUFEUkIE
MQswCQYDVQQGEwJFUzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANzNzbG/3iX1/xwz
c5k8G6F9aDEiZs4Zo0J3wNsVzW0E0H+41/mIgRYGLIOaTMEP5XH2U7/MzSnMkAyk1F+ga8lQ1wd
/XoXC2IfZ2dit0PIWCWASqGYkDnTxBbKUkmq018oatbYTGBHmpkIE0tr+Ese0dVD4texbIb2/7Rw
VfYImbd0AcDznrV85ASICFBZeE8aINvvyMmJ0ze48z2G0RnLg1oQBwhPmXQCB/AyUcj75tA8InZ9
cn6sdjfBinUgXEDchD/QSXxNZ6457+T0gOHKneYtqy7mEpXa+fvf4+KMPYf7RW5Eq/Z4kicUoV1r
T3B7V3Pv+V2oD3WI7xFgGYSwZEDu2KmG+qXXRfQRb/GGyDRbiEjOut3Nm92HwE26Ksxq6BILsOB7
kB6FC0mJAfb/gt9YZSKDSNYH0Bxm/GYoOsTD5fiZZSdSWPNz8W8CRIR10KTjaFNhcu/2L6mzzPX0
9tBc3GlMzHnSpBvIcwY0dLTxasopKMc0bFsg2LoAjMwJwcdvXQSrt08md6k1zyDWs8xadA0+yXs
aJYKot2DH8o8j3Q2VTv9Rh7wiQx0fuCBK4Egtb1Ailx4ZIxdI7bqnEdxDvGYiZshjwjVesp0R+r
yh5j57NztKe4Kjr2H/uHZYj885/+v+vVHbaoA+llgxmM4BjtF9gcDT2cilh/AgMBAAGjggMBMIIC
/TA3HggrBgEFBQcBAQQrMCkwJwYIKwYBBQUHMAGGG2h0dHAo6Ly9YS5tdGluLmVzL210aW4vb2Nz
cDAOBgNVHQ8BAf8EBAMCAQYwGwYDVR0RBBQwEoEQYWRtaW5fY2FAbXRpbc5lczAbBgNVHRIEFDAS
gRBhZGI1pbl9jYUBtdGluLmVzMA8GA1UdEwEB/wQFMAMBAf8wcgYDVR0fBGswATAyoDCgLoYsaHR0
cDovL2NhL m10aW4uZXMvbXRpbi9jcmwvTVRJTkF1dG9yaWRhZFJhaXowM6AxoC+GL Wh0dHA6L y9j
YTlubXRpbi5lcy9tdGluL2NybC9NVEIOQXV0b3JpZGFkUmFpejCBuQYDVR0gBIGxMIGuMIGrBgsr
BgEEAYHZIBQIEATCBmzAwBggrBgEFBQcCARYkaHR0cDovL2NhL m10aW4uZXMvbXRpbi9EUENSUG9s
aXRpY2FzMGcGCCsGAQUFBwICMFsaWUNlcnRpZmljYWRvIHJh7XouIENvbnN1bHRlIGxhcyBjb25k
aWNpb25lcyBkZSB1c28gZW4gaHR0cDovL2NhL m10aW4uZXMvbXRpbi9EUENSUG9saXRpY2FzMB0G
A1UdDgQWBBQzQxizxEsdyx/S8E7830rkFWDIgzCCARYGA1UdIwSCAQ0wggEJgBQzQxizxEsdyx/S
8E7830rkFWDIgo6GB6KSB51CBtjEWMBQGA1UEAxMNQUMxIEBSVoqTVRJTjESMBAGA1UEBRMJUzJ4
MTkwMDFFMTUwMwYDVQQLEyxQUkVTVEFET1IgREUgU0VSVkIDSU9TIERFIENFUlRJRkIDQUNJT04g
TVRJTjExMC8GA1UECxMoU1VCREISRUNDSU9OIEdFTkVSQUwgREUgUFJPQ0VTTyBERSBEQVRPUzEs
MCoGA1UECbMjTUlOSVNURVIJTyBERSBUUkFCQUpPIEUgSU5NSUdSQUNJT04xDzANBgNVBAcTBk1B
RFJBRDELMAkGA1UEBhMCRVOCBgULQV6CzzANBgkqhkG9w0BAQUFAAOCAgEAmzQqDpHTkqnq/0Rn
06AtIGfzEA8aN3ddUkhmarj3iPOCwyr0YQ0sny+GLWHpYFm9t0+vkwkc+TN3QJyhfGXcXpCVqtS+
gvT8gh0exT3gXK7eLdVjdqvx7CSnlPge6M9xggPdjnZiKrUpiBMkrVz0oEq46hOKVo1qL2g5coZY
xKSrdXxE5xqEDI0R3Bm5HDbu8/9Rm7NDyCV+5w5Io+RPBi0VHqCmR5BXO/gvLdsjuusjk7C4L/htg
HNQZsG14j0udpnsoZ0tdeEi9sT6Y1LsVr/NbR11yB7PD65KGl2HLAZ0bAqFUyReesmgfHGbk41v
SH+2WHGyTKYaCSM0UHEVa0tb+7abcKMCRHLCyAtZO3q8YZuYNYuojpBpw76ns570TFQLzib1fz
A8oomRrAVWB1e2O+ZD+WTkuP/S2mdMDfSTrsVX5m07r97SOxY/JbP+12odnTDP4ubwqmU0vv0fNH
rbke7EwfvtCDU8ObFUX/LgfR2mqSReZsV1skLlFpyTDP1/ukATVazafrFG+0t2AtCMVxyJPivvVf
9Qz6WFE9e8gvN/mTHCoJ4Gf9IoICyus2sNYbplAPWp12/6RPxunNxOHQ51g+1nnAd00M1bPkmE3d
R15SsOIPDUlZpRAkUn+YjVCOcl6lh/u5ktZPyRzr78iS2by2w818TcdoCQ=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *ES*

Issuer L: *MADRID*

Issuer O: *MINISTERIO DE TRABAJO E INMIGRACION*

Issuer OU: *SUBDIRECCION GENERAL DE PROCESO DE DATOS*

Issuer OU: *PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*

Issuer SERIAL NUMBER: *S2819001E*

Issuer CN: *AC1 RAIZ MTIN*

Subject C: *ES*

Subject L: *MADRID*

Subject O: *MINISTERIO DE TRABAJO E INMIGRACION*

Subject OU:	*SUBDIRECCION GENERAL DE PROCESO DE DATOS*
Subject OU:	*PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*
Subject SERIAL NUMBER:	*S2819001E*
Subject CN:	*AC1 RAIZ MTIN*
Valid from:	*Thu Nov 05 17:17:45 CET 2009*
Valid to:	*Sun Nov 03 17:17:45 CET 2019*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DC:CD:CD:B1:BF:DE:25:F5:FF:1C:33:73:99:3C:1B:A1:6D:F5:A0:C4:7D:9B:38:66:8D:09:DF:03:6C:57:35:B4:13:41:FE:E3:5F:E6:22:04:58:18:B9:4E:69:33:04:3F:95:C7:D9:4E:FF:33:34:A7:32:40:32:93:57:FE:81:AF:25:43:5C:1D:FD:7B:57:0B:62:08:67:67:62:B4:E3:E5:58:25:80:E6:AA:86:62:40:E7:4F:10:61:29:49:26:AB:4D:7C:A1:AB:5B:61:31:81:06:6A:64:94:4D:27:F8:4B:1E:D1:D5:43:E2:D7:B1:6D:F6:F6:FF:B4:70:55:F6:08:99:B7:74:01:E0:F3:9E:B5:7C:E4:04:88:08:50:59:78:1F:1A:94:DB:EF:C8:C9:89:D3:37:B8:F3:3D:86:D1:19:CB:83:5A:10:07:08:4F:99:74:02:07:F0:32:51:C8:FB:E6:D0:3C:26:76:7D:72:7E:AC:76:37:C1:8A:75:20:5C:40:DC:84:3F:D0:49:7C:4D:67:AE:39:EF:E4:CE:80:E1:CA:9D:E6:2D:AB:2E:E6:12:95:DA:F9:FB:DF:E3:E2:8C:3D:87:FB:45:6E:44:AB:F6:78:92:27:14:A1:5D:6B:4F:70:7B:57:73:EF:F9:5D:A8:0F:75:9F:EF:11:60:19:84:B0:64:40:EE:D8:A9:86:FA:A5:D7:45:F4:11:6F:F1:86:C8:34:5B:88:48:CE:BA:DD:CD:9B:DD:88:E3:01:36:E8:AC:6A:E8:12:0B:B0:E0:7B:90:1E:85:0B:49:89:01:F6:FF:82:DF:58:65:22:83:48:D6:07:D0:1C:66:FC:66:28:3A:C4:C3:E5:F8:99:65:27:52:58:F3:6B:F1:6F:02:44:84:75:D0:A4:E3:68:53:61:72:EF:F6:2F:A9:B3:AC:F5:F4:F6:D0:5C:DC:69:4C:CC:79:D2:A4:1B:C8:73:06:34:74:B4:F1:6A:CA:29:28:C7:34:84:5B:23:D8:BA:00:8C:CC:09:C1:C7:6F:5D:04:AB:B7:4F:26:77:A9:35:CF:20:D6:B3:FF:31:69:D0:34:FB:25:EC:68:96:0A:A2:DD:83:1F:CA:3C:8F:74:36:25:54:EF:F5:18:7B:C2:24:31:D1:FB:82:04:AE:04:82:D6:F5:02:29:71:E1:92:71:74:8E:DB:AA:71:1D:C4:3B:C6:62:26:6C:86:3C:23:55:EB:29:D1:1F:AB:CA:1E:63:E7:B3:73:B4:A7:B8:2A:3A:F6:1F:FB:87:65:88:FC:F3:9F:FE:BF:EB:D5:1D:B6:A8:03:E9:65:83:19:8C:E0:18:ED:17:D8:1C:0D:3D:9C:8A:58:7F:02:03:01:00:01*
Authority Info Access	*http://ca.mtin.es/mtin/ocsp*
Subject Alternative Name	*admin_ca@mtin.es*
Issuer Alternative Name	*admin_ca@mtin.es*
Basic Constraints	*IsCA: true*
CRL Distribution Points	*http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz* *http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.27781.2.4.1* *CPS pointer: http://ca.mtin.es/mtin/DPCyPoliticas* *CPS text: [Certificado raíz. Consulte las condiciones de uso en http://ca.mtin.es/mtin/DPCyPoliticas]*
Subject Key Identifier	*33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83*
Authority Key Identifier	*33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*5B:1D:9D:24:DE:0A:FE:A8:B3:5B:A0:4A:1C:3E:25:D0:81:2C:DF:7C:46:25:DE:0A:89:AF:9F:E4:BB:D1:BB:15*

X509SubjectName

Subject C:	*ES*
Subject L:	*MADRID*
Subject O:	*MINISTERIO DE TRABAJO E INMIGRACION*

Subject OU: *SUBDIRECCION GENERAL DE PROCESO DE DATOS*

Subject OU: *PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*

Subject SERIAL NUMBER: *S2819001E*

Subject CN: *AC1 RAIZ MTIN*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-05-07T00:00:00Z*

Scheme Service Definition URI

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

19.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3*

19.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

19.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por la AC1 RAIZ MTIN*
Name	*[en]*	*Qualified Certificates issued by AC1 RAIZ MTIN*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*MADRID*
Subject O:	*MINISTERIO DE TRABAJO E INMIGRACION*
Subject OU:	*SUBDIRECCION GENERAL DE PROCESO DE DATOS*
Subject OU:	*PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*
Subject SERIAL NUMBER:	*S2819001E*
Subject CN:	*AC1 RAIZ MTIN*

X509SKI

X509 SK I	*M0MYs8RLHcsf+fBO/N9K5BVgyIM=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

19.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3*

19.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

19.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por la AC1 RAIZ MTIN

Name [en] Qualified Certificates issued by AC1 RAIZ MTIN

Service digital identities

X509SubjectName

Subject C: ES

Subject L: MADRID

Subject O: MINISTERIO DE TRABAJO E INMIGRACION

Subject OU: SUBDIRECCION GENERAL DE PROCESO DE DATOS

Subject OU: PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN

Subject SERIAL NUMBER: S2819001E

Subject CN: AC1 RAIZ MTIN

X509SKI

X509 SK I M0MYs8RLHcsf+fBO/N9K5BVgyIM=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2010-12-21T00:00:00Z

19.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3*

19.2 - Service (granted): SUBCA1 MEYSS

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *SUBCA1 MEYSS*

Name *[es]* *SUBCA1 MEYSS*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1480675521*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIKDjCCB/agAwIBAgIEWEFQwTANBgkqhkiG9w0BAQsFADCCAQsxCzAJBgNVBAYTAkVTMQ8wDQYD
VQQHDAZNQURSSUQxMDAuBgNVBAoMJ01JTkITVESSU8gREUgRU1QTEVPIFkgU0VHVVJIREFEIFNP
Q0lBTDE/MD0GA1UECww2Uy5HLiBERSBURUNOT0xPR0lBUyBERSBMQSBJTkZPUk1BQ0lPTiBZIENP
TVVOSUNBQ0lPTkVTMTIwMAYDVQQLDCIQUkVTVEFET1lgREUgU0VSVkIDSU9TIERFIENPTkZJQU5a
QSBNRVITUzESMBAGA1UEBRMJUzI4MTkwMDFFMRgwFgYDVQRhDA9WQVRFUy1TMjgxOTAwMUUxFjAU
BgNVBAMMDUJDIEJBSVogTUVZUlMwHhcNMTYxMjAyMTEyNjI5WhcNMzYxMjAyMTEiNjI5WjCCAQox
CZAJBgNVBAYTAkVTMQ8wDQYDVQQHDAZNQURSSUQxMDAuBgNVBAoMJ01JTkITVESSU8gREUgRU1Q
TEVPIFkgU0VHVVJIREFEIFNPQ0lBTDE/MD0GA1UECww2Uy5HLiBERSBURUNOT0xPR0lBUyBERSBM
QSBJTkZPUk1BQ0lPTiBZIENPTVVOSUNBQ0lPTkVTMTIwMAYDVQQLDCIQUkVTVEFET1lgREUgU0VS
VkIDSU9TIERFIENPTkZJQU5aQSBNRVITUzESMBAGA1UEBRMJUzI4MTkwMDFFMRgwFgYDVQRhDA9W
QVRFUy1TMjgxOTAwMUUxFTATBgNVBAMMDFNVQkNBMSBNRVITUzCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBANEwz34UgxhX6foXjTagj9QXm/blDqcz1HK6Uj/LpuEAZH/6myphOWM+JtBy
3H4ULHy977ZlF7vTwUbAlnzlJZvUnzEWQ+145/y8QSDwehBXt3EYU3CTbcNYxJoKMR54I4EY8Ke
lj0IHWhsw8T/t3oZzNwugqwz0EgSJR9toyXZ1r0jQ4uVY32Pjdq3Jvr2UcsV01expnbmP2MBSGs
Uqa4MGZVSmfZkH6cPhqkr9N45IcyqCktIfCYtNXOEVAvYmB72PkcDXQWRzn0XUn2kuPWcUsXQv1
fM/0aggc/CoWKgBx0DgYDqWAcg677oHgZImUjQN9SoHJ9rDvS0a/BTtdmY+hZft1B9xInjl2qkYB
FQwZ6SNy70fua21IrWLYcPAzxsguo2n8rIyve5VMtnrzLxaUc7jBGlcz3shm0u+ukLzR1TncKk5c
8VOFj+CgVce0n/LIU/6+ehWE0ta0W/KNs/PQ3qe0GalrZR86+BR2OMqFNTqRt3PSf/MyMC1Ps4F9R4
MasKcyzjLxWCpb6kCQ3Ifnal+EDrpXEkG99vbD0F43UND1GT0GeRVKMMJrx1cus9mTuzLVbgAt5rZ
wqEvY6tZqj+9kj53297H5kY+S1NdrYTJmP61KN8RHABsvJTWiJ6zupZ65dwAaiHo1HKhNHcNYQA
p7d6uSIvT4aFAw11AgMBAAGjggN1MIIDcTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB
/zB2BggrBgEFBQcBAQRqMGgwLgYIKwYBBQUHMAGGIlmhldHA6Ly9YS5lbXBsZW8uZ29LmVzL211
cXNzL29jc3AwNgYIKwYBBQUHMAKGKmh0dHA6Ly9YS5lbXBsZW8uZ29LmVzL21lcXNzL2NlcnRp
ZmljYWRvczCB4wYDVR0gBIHbMIHYMIHVBgwrBgEEAYHZBQIFAQEwgcQwNwYIKwYBBQUHAgEWK2h0
dHA6Ly9YS5lbXBsZW8uZ29iLmVzL211eXNzL0RQQ3lQb2xpdGlJYXMwgYgGCCsGAQUFBwICMHwa
ckNlcnRpZmljYWRvJGRlIEFDIFN1Ym9yZGluYWRhIFNVQkNBMSBNRVITUy4gQ29uc3VsdGUgbGFz
IGNvbmRpY2hvbmVzIGRlIHVzbyBlbiBodHRwOi8vY2EuZWIwbGVvL mdvYi5lcy9lZXlzcy9EUENS
UG9aXRpY2FzMIIBrgYDVR0fBIIBpTCCAaEwcaBvoG2GNGh0dHA6Ly9YS5lbXBsZW8uZ29LmVz
L21leXNzL2NybC9NRVITU0F1dG9yaWRhZFlhaXqGNWh0dHA6Ly9YTlaZW1wbGVvLmdvYi5lcy9t
ZXlzcy9jcmwv1UVZU1NBdXRvcmlkYWRSYW16MIIBKqCCASagggEipI1BHjCCARoxCzAJBgNVBAYT
AkVTMQ8wDQYDVQQHDAZNQURSSUQxMDAuBgNVBAoMJ01JTkITVESSU8gREUgRU1QTEVPIFkgU0VH
VVJIREFEIFNPQ0lBTDE/MD0GA1UECww2Uy5HLiBERSBURUNOT0xPR0lBUyBERSBMQSBJTkZPUk1B
Q0lPTiBZIENPTVVOSUNBQ0lPTkVTMTIwMAYDVQQLDCIQUkVTVEFET1lgREUgU0VSVkIDSU9TIERF
IENPTkZJQU5aQSBNRVITUzESMBAGA1UEBRMJUzI4MTkwMDFFMRgwFgYDVQRhDA9WQVRFUy1TMjgx
OTAwMUUxFjAUBgNVBAMMDUJDIEJBSVogTUVZUlMxHDTALBgNVBAMMBENSTDEwHwYDVR0jBBgwFoAU
f7cr8i62D6wFOKdjL9YTw4a9XEwHQYDVR0OBBYEFJ6LHbP6BYuB1+pZ6Lp952ISALzMA0GCSqG
SIb3DQEBCwUAA4ICAQAZActCZIEZybemYHZC1Jf3IjZwRiNPlUk5aAyAs27I3yHgWV3qVgXFWYnu
e37QobFxOOAT1EfisiWhwKdMtq8hjK4FB8YWwVR8c42iMadingnMKmm8ZAJZScnemBdwhuajrxiT
486sa16vaQrY7mW2s9PWbJTYlI4sf6L+4MdI/XQb317NXpqok2WHfOtSS/LDxeIc09Bw1ikUDSc
Gawr+4uCLCExxw4I2vIGHEcxasy5vTNpTGavlRqsLaXGVy6sC6n0UXMT9DB1sfQRwTJCfxmdIp
jQoFZ1iNcw3ErL V/qRpacnCMICkBHdqtszcq2MIyx5Ct148EULrT0iv+HpR/n96ovWC40N7L+Yob
1nrdYejX7uNJpoFI2KgcmH1zLM2ih7D+ZrDsdz1Pq+FTnPbVPdljbjpBIfingwT4F4GZsOJ2pIHsc
TKhzA8LTfL+DzlHJBKQ4VXsZSNZkrmwT8OVNM6vFJdLRfmgbb0HRvMD98eDoJINnwuQ4s2+4QbW
19HEWjvHg4z+OkTFdwV0bNR9j7wLs6d3LhOh/0XFiE2aJs3Pk2IPjQ7dzr0Yp61Bik2/wrs4zcKb
0A Q0LiigLU2dU8HrK5Devz738C5feVJ4qbN7EwtiwLDu3X6cnvds1bxqWDISTKXaaJyMvxi7h2tO
cccCxhpK1gKT5oa/Kw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *AC RAIZ MEYSS*

Issuer 2.5.4.97: *VATES-S2819001E*

Issuer SERIAL NUMBER:	*S2819001E*
Issuer OU:	*PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*
Issuer OU:	*S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*
Issuer O:	*MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*
Issuer L:	*MADRID*
Issuer C:	*ES*
Subject CN:	*SUBCA1 MEYSS*
Subject 2.5.4.97:	*VATES-S2819001E*
Subject SERIAL NUMBER:	*S2819001E*
Subject OU:	*PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*
Subject OU:	*S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*
Subject O:	*MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*
Subject L:	*MADRID*
Subject C:	*ES*
Valid from:	*Fri Dec 02 12:26:29 CET 2016*
Valid to:	*Tue Dec 02 12:56:29 CET 2036*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:30:CF:7E:14:83:18:57:E9:FA:17:8D:36:A0:8F:D4:17:9B:F6:E5:0E:A7:33:D4:72:BA:52:3F:CB:A6:E1:00:64:7F:FA:9B:2A:61:39:63:3E:26:20:72:DC:7E:14:2C:7C:BD:EF:B6:65:23:EE:EF:4F:05:1B:02:59:F3:25:9B:D4:9F:31:16:43:ED:78:E7:FC:BC:43:90:F0:7A:10:57:B7:71:18:53:70:93:6D:C3:58:C6:22:68:28:C4:79:E0:8E:04:63:C2:9E:96:3D:07:5A:1B:30:F0:5F:ED:FF:7A:19:CC:DC:2E:82:AC:33:D0:48:12:25:1F:6D:A3:25:D9:D6:BD:23:43:8B:8D:63:7D:8F:8D:DA:B7:26:FA:F6:51:CB:15:8B:4D:5E:C6:99:DB:98:FD:8C:05:21:AC:52:A6:B8:30:66:55:4A:61:76:90:7E:9C:3E:1A:A4:AF:D3:78:4B:89:5C:CA:A0:A4:B4:70:98:B4:D5:CE:11:50:2F:62:60:7B:D8:F9:1E:0D:74:16:47:39:CE:89:75:27:DA:4B:8F:59:C5:2C:5D:0B:E5:7C:CF:F4:6A:08:1E:FC:2A:16:2A:00:71:D0:38:18:0E:A5:80:7A:0E:BB:EE:81:E0:64:89:94:8D:03:7D:4A:81:C9:F6:B0:EF:4B:46:BF:05:3B:5D:99:8F:A1:65:FB:75:07:DC:48:9E:39:76:AA:46:01:15:0C:19:E9:23:72:EF:47:EE:6B:64:DF:AD:62:D8:78:F0:33:C6:C8:2E:A3:69:FC:AC:8C:AF:7B:95:4C:B6:7A:F7:2F:16:94:73:BB:C1:1A:57:B3:DE:C8:66:D2:EF:AE:90:BC:D1:D5:39:DC:2A:4E:5C:F1:53:85:96:3F:86:81:57:1E:D2:7F:CB:95:4E:BE:7A:15:84:D1:A3:96:FC:A3:6C:FC:F4:37:A9:E3:86:6A:5A:D9:47:CE:BE:05:1D:8E:32:A1:4D:4E:A4:6D:DC:F4:9F:33:23:02:D4:FB:38:17:D4:78:31:AB:0A:73:2C:E3:2F:15:82:A5:BE:A4:09:0D:DF:9D:A2:3E:10:3A:E9:5C:49:06:F4:9B:DB:0E:5D:05:E3:75:0D:0F:51:93:D0:67:91:54:A3:0C:8F:1D:5C:BA:CF:66:4E:EC:CB:56:18:00:8B:9A:D9:C2:A1:2F:63:AB:49:CE:A8:FE:F6:48:F9:DF:6F:7B:1F:99:18:F9:2D:4D:76:B6:13:26:63:FA:D4:A3:7C:44:70:01:B2:F2:53:5A:22:7A:CE:EA:59:EB:97:70:01:A8:87:A3:51:CA:84:D1:DE:35:84:00:A7:B7:7A:B9:22:2F:4F:86:9F:03:0D:75:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Authority Info Access	*http://ca.empleo.gob.es/meyss/ocsp* *http://ca.empleo.gob.es/meyss/certificados*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.27781.2.5.1.1* *CPS pointer: http://ca.empleo.gob.es/meyss/DPCyPoliticas* *CPS text: [Certificado de AC Subordinada SUBCA1 MEYSS. Consulte las condiciones de uso en http://ca.empleo.gob.es/meyss/DPCyPoliticas]*

CRL Distribution Points	*http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz* *http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz* *C=ES,L=MADRID,O=MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL,OU=S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES,OU=PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS,SERIALNUMBER=S2819001E,2.5.4.97=VATES-S2819001E,CN=AC RAIZ MEYSS,CN=CRL1*
Authority Key Identifier	*7F:B7:2D:F2:2E:B6:0F:AC:05:38:A7:63:2F:D6:3F:4F:0E:1A:F5:71*
Subject Key Identifier	*9E:8B:1D:B3:FA:07:2B:81:D7:EA:59:E8:B9:69:F7:9D:B5:48:02:E2*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*24:E0:BA:DA:DA:29:05:5C:66:22:CA:23:74:A2:28:A4:71:A4:D2:4C:2D:54:71:88:E3:8F:07:1A:9D:14:60:88*

X509SubjectName

Subject CN:	*SUBCA1 MEYSS*
Subject 2.5.4.97:	*VATES-S2819001E*
Subject SERIAL NUMBER:	*S2819001E*
Subject OU:	*PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*
Subject OU:	*S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*
Subject O:	*MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*nosds/oHK4HX6lnouWn3nbVIAuI=*

Service Status		*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Service status description	*[en]*	*undefined.*
	[es]	*undefined.*
Status Starting Time		*2018-05-07T00:00:00Z*

19.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

19.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

19.2.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] SUBCA1 MEYSS

Name [es] SUBCA1 MEYSS

Service digital identities

X509SubjectName

Subject CN: SUBCA1 MEYSS

Subject 2.5.4.97: VATES-S2819001E

Subject SERIAL NUMBER: S2819001E

Subject OU: PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

Subject OU: S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

Subject O: MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Subject L: MADRID

Subject C: ES

X509SKI

X509 SK I nosds/oHK4HX6lnouWn3nbVIAuI=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2018-05-07T00:00:00Z

19.2.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

19.3 - Service (granted): SUBCA2 MEYSS

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *SUBCA2 MEYSS*

Name *[es]* *SUBCA2 MEYSS*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1480675522*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIKDjCCB/agAwIBAgIEWEFQwjANBgkqhkiG9w0BAQsFADCCAQsxCzAJBgNVBAYTAkVTMQ8wDQYD
VQQHDAZNQURSSUQxMDAuBgNVBAoMJ01JTkITVEVSSU8gREUgRU1QTEVPIFkgU0VHVVJREFEIFNP
Q0lBTDE/MD0GA1UECww2Uy5HLiBERSBURUNOT0xPR0lBUyBERSBMQSBJTkZPUk1BQ0IPTiBZIENP
TVVOSUNBQ0lPTkVTMTIwMAYDVQQLDCIQUkVTVEFET1IgREUgU0VSVkIDSU9TIERFIENPTkZIQUSa
QSBNRVITUzESMBAGA1UEBRMJUzI4MTkwMDFFMRgwFgYDVQRhDA9WQVREUyITMjgxOTAwMUUxFjAU
BgNVBAMMDUFDIFJBSVog1UVZU1MwHhcNMTYxMjAyMTE1MjQ5WhcNMzYxMjAyMTIyMjQ5WjCCAQox
CzAJBgNVBAYTAkVTMQ8wDQYDVQQHDAZNQURSSUQxMDAuBgNVBAoMJ01JTkITVEVSSU8gREUgRU1Q
TEVPIFkgU0VHVVJREFEIFNPQ0lBTDE/MD0GA1UECww2Uy5HLiBERSBURUNOT0xPR0lBUyBERSBM
QSBJTkZPUk1BQ0IPTiBZIENPTVVOSUNBQ0lPTkVTMTIwMAYDVQQLDCIQUkVTVEFET1IgREUgU0VS
VkIDSU9TIERFIENPTkZIQUSeQSBNRVITUzESMBAGA1UEBRMJUzI4MTkwMDFFMRgwFgYDVQRhDA9W
QVREUyITMjgxOTAwMUUxFTATBgNVBAMMDFNVQkNBMiBNRVITUzCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBAKYmZWoVvUbc7qrQGgzu2SEg2rYoGJ6EIGdgfV53Ps9OjpsoKuFwQSynfcLA
+qfxpRWxZFpTuAqUe/ie7AIDbLuPN7ARpR9PIgr+XH4osLEu6uILsHG3BBZ7X269qUJSURlBIwFWs
Q62OKKKkELFBfVuXcyDxLZ2pWUQkHILESd0XVHAt7bxgIzGiDU55SwAzauMXNLZ8QZRFWIzqBhO
ZdYZGezjyy/V9gVbOZDE3A5fBlxcht9bP0rAZxHj0waQ3VOUSOaVzims/QWzEPlU90HeRHVayxGs
XEdreQcnXEBOzQ6yD5cSLknXnCoCmq4lHyTUblKnF8Vgy1wyOC6RaYJ0qy5AvE52FOIQIKkZURY1
SJqUKpVnztKVjSjW08q63IdkAsBdw7biFoJv1YDNVr1n6RsNpGA1HGA42BiFSKUWp0Hi6yII9HSLoc
8LIVm8YIYIa1YuiNuTs9zCSaSdIXz2APOhjhqBtOrk65IYhYysJBbSCuuLeB10ecSyHxEoSHjI
d6KKg2bwqSPS/yCak7z1o9VABAowKxcnWZkZ9h5r6g1XrRfyQ/BQF9UeKAWKBKlNNMScEZNPX18k
drRqydiqoVsc/8uxHSXvhqG8TeXZ/CGNi9pMWGgwbU/h2pX2fynLZ84HUMtYH4h0XnD4Q56YgwYLq
Yqfik0t0BkRX0RTpAgMBAAGjggNIMIIDcTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB
/zB2BgrBgEFBQcBAQRqMGgwLzYIKwYBBQUHMAGGImhtdHA6Ly9YS5lbXBsZW8uZ29iLmVzLZ11
eXNzZ29jc3AwNgYIKwYBBQUHMAKGKmh0dHA6Ly9YS5lbXBsZW8uZ29iLmVzL21leXNzL2NlcnRp
ZmljYWRvczCB4wYDVR0gBIHbMIHYMIHVBgwrBgEEAYHZBQIFAQIwgcQwNwYIKwYBBQUHAgEWK2h0
dHA6Ly9YS5lbXBsZW8uZ29iLmVzL21leXNzL0RQQ3lQb2xpdGlyYXMwgYgGCCsGAQUFBwICMHwa
ckNlcnRpZmljYWRvcGRlIEFDIM1Ym9yZGlzYWRhIFNVQkNiMiBNRVlTUy4gQ29ac3VsdGIgbGFz
IGNvbmRpY2lvbmVzIGRlIHVzbyBlbiBodHRwOi8vY2EuZW1wbGVvLmdvYi5ley9tZXlzcy9EUEN5
UG9saXRpY2FzMIIBrgYDVR0fBIIBpTCCAaEwcaBvoG2GNGh0dHA6Ly9YS5lbXBsZW8uZ29iLmVz
L21leXNzL2NybC9NRVITU0F1dG9yaWRhZFlhaXqGNWh0dHA6Ly9YTluZW1wbGVvLmdvYi5ley9t
ZXlzcy9jcmwvTUVZU1NBdXRvcmlkYWRSYW16MIIBKqCCASaggeEipIIBHjCCARoxCzAJBgNVBAYT
AkVTMQ8wDQYDVQQHDAZNQURSSUQxMDAuBgNVBAoMJ01JTkITVEVSSU8gREUgRU1QTEVPIFkgU0VH
VVJREFEIFNPQ0lBTDE/MD0GA1UECww2Uy5HLiBERSBURUNOT0xPR0lBUyBERSBMQSBJTkZPUk1B
Q0IPTiBZIENPTVVOSUNBQ0lPTkVTMTIwMAYDVQQLDCIQUkVTVEFET1IgREUgU0VSVkIDSU9TIERF
IENPTkZIQUSaQSBNRVITUzESMBAGA1UEBRMJUzI4MTkwMDFFMRgwFgYDVQRhDA9WQVREUyITMjgx
OTAwMUUxFjAUBgNVBAMMDUFDIFJBSVog1UVZU1MxDTALBgNVBAMMBENSTDEwHwYDVR0jBBgwFoAU
f7ct8i62D6wFOKdjL9Y/Tw4a9XEwHQYDVR0OBBYEFHtkD1FhphsneOJ9uDkPXIM/ZYCMA0GCSqG
SIb3DQEBCwUAA4ICAQAFwgFzQ7AWKhiqv1qRE65huet9/a15xzNYIMBJSaKctizhoYyRAc23DlnS
OdPbuQUB+rzDpgisLcF3n/wk96mQ/ayjGGoX+tHBfgIXJFArpDaWHsJAuoEIQlig96jIHaKVL/1R
r3jZBqaN+FFT4kJlFuOXjmoPDTcC/cbja3wl/EJDFVLpSsHCEJbo610NdlCXCRSWYg+wg4AkPBbSl
DG2NMCHiYuvtgvB4pRKoE/JuRcTLeM2lt7LSZOHNXubw486JZ2H1jhZR9eB8wIO25VPTwJJQvFS4
6IrVFn7nMlNgsG8h7uQysTJLcxVXhqH03wtJIrwFjeIaZGcUc9jIWVJ5RGfAdgp4/7dTHxcCSDa/
LZ/nwpCQ/HENdOKm316w/9LGW1KPEWteHZ1uksD0oX6o4Yi3EPrmKC/Sae2PXzcnMZcJxGwSUIA
17qcX4+WYTM6+jfToKuNn5g/GzSY23PPMc/67GqjH8+V9+QTOLWZVJbbvsp1UB/ABtLbsfoMr1
In7gxA8gJhXw0E6yE3G9Rdpz1MczSwCZ0IacbK7LgCICQTtPGvRBYtBZYvbEHMLlgHERUhmkerYq
aUfbzCOUjP+3ts8pC61/1cq9COuYBE4QsKCmlMpdTHrFHyJL7E7S2NiEPiJy1U61bXbQUnVOnY8ye
ubOFS3Ogt0xPmO/+ug==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *AC RAIZ MEYSS*

Issuer 2.5.4.97: *VATES-S2819001E*

Issuer SERIAL NUMBER:	*S2819001E*
Issuer OU:	*PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*
Issuer OU:	*S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*
Issuer O:	*MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*
Issuer L:	*MADRID*
Issuer C:	*ES*
Subject CN:	*SUBCA2 MEYSS*
Subject 2.5.4.97:	*VATES-S2819001E*
Subject SERIAL NUMBER:	*S2819001E*
Subject OU:	*PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*
Subject OU:	*S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*
Subject O:	*MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*
Subject L:	*MADRID*
Subject C:	*ES*
Valid from:	*Fri Dec 02 12:52:49 CET 2016*
Valid to:	*Tue Dec 02 13:22:49 CET 2036*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:26:65:6A:15:BD:46:DC:EE:AA:D0:1A:0C:EE:D9:21:20:DA:B6:28:18:9E:84:20:67:60:7D:5E:77:3E:CF:4E:8E:9B:28:2A:E1:70:41:2C:A7:7D:C2:C0:FA:A7:F1:A5:15:B1:64:5A:53:B8:0A:94:89:E4:C0:7C:36:CB:B8:F3:7B:01:1A:51:F4:F2:20:AF:E5:C7:E2:8B:0B:12:EE:AE:7C:BB:07:1B:70:41:67:B5:F6:EB:DA:B5:27:74:94:46:50:48:C0:55:AC:43:AD:8E:24:62:8A:90:42:C5:06:D4:EF:53:17:32:0F:12:F6:66:95:94:42:41:E5:2C:44:9D:D1:75:47:01:FE:E1:C6:09:73:1B:F0:D4:E5:2C:00:CD:AB:8C:5C:D2:D9:F1:06:51:15:62:33:A8:18:4E:65:D6:19:19:EC:E3:CB:2F:D5:F6:05:5B:39:90:C4:DC:0E:5F:04:8C:5C:86:DF:5B:3F:4A:C0:67:11:E3:D3:06:90:DD:53:94:48:E6:95:CE:29:AC:FD:05:B3:10:F9:54:F7:41:DE:44:75:5A:CB:11:AC:5C:47:6B:79:07:27:5C:40:4E:CD:0E:B2:0F:97:12:2E:49:D7:9C:2A:02:9A:AE:25:1F:24:D4:6E:52:A7:17:C5:60:C8:8C:32:38:2E:91:69:82:74:AB:2E:40:BC:4E:76:15:09:50:94:A9:19:51:16:08:48:9A:94:2A:95:67:CD:F2:95:8D:28:D6:D3:CA:BA:DE:22:24:02:C0:5D:C3:B6:E2:16:82:6F:D5:80:D7:56:BD:67:E9:1B:0D:A4:60:07:18:0E:36:06:21:52:29:45:A9:D0:7E:B2:20:8F:47:48:BA:1C:F0:B9:55:B6:7F:18:95:89:5A:D5:8B:A2:36:E4:EC:F7:30:92:B9:27:48:5F:30:36:00:F3:AD:8E:1A:81:B4:EA:E4:EB:99:58:85:8C:92:24:1B:39:0A:EB:8B:78:1D:74:79:E4:B2:1F:11:28:48:78:C8:77:A2:8A:83:66:F0:A9:23:D2:FF:20:9A:93:BC:F5:A3:D5:40:04:0A:30:2B:17:27:59:99:19:F6:1E:6B:EA:0D:57:AD:17:F2:43:F0:50:17:D5:1E:28:05:8A:04:A9:4D:34:C4:9C:11:93:4F:5F:5F:24:76:B4:6A:C9:D8:AA:A1:5B:1E:FF:CB:B1:1D:25:EF:86:A1:BC:4D:E5:D9:FC:21:8D:8B:DA:4C:58:68:30:85:48:76:A5:7D:9F:CA:72:D9:F3:81:D4:32:D6:07:E2:1D:17:9C:3E:10:E7:A6:20:C1:82:EA:62:A7:E2:93:4B:74:06:44:57:D1:14:E9:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Authority Info Access	*http://ca.empleo.gob.es/meyss/ocsp* *http://ca.empleo.gob.es/meyss/certificados*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.27781.2.5.1.2* *CPS pointer: http://ca.empleo.gob.es/meyss/DPCyPoliticas* *CPS text: [Certificado de AC Subordinada SUBCA2 MEYSS. Consulte las condiciones de uso en http://ca.empleo.gob.es/meyss/DPCyPoliticas]*

CRL Distribution Points	*http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz* *http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz* *C=ES,L=MADRID,O=MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL,OU=S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES,OU=PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS,SERIALNUMBER=S2819001E,2.5.4.97=VATES-S2819001E,CN=AC RAIZ MEYSS,CN=CRL1*
Authority Key Identifier	*7F:B7:2D:F2:2E:B6:0F:AC:05:38:A7:63:2F:D6:3F:4F:0E:1A:F5:71*
Subject Key Identifier	*72:2D:90:3D:45:86:98:6C:9D:E3:89:F6:E0:E4:3D:77:CC:FD:96:02*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*18:70:4F:60:CC:F3:59:4C:89:9A:DA:8B:E4:D4:D3:D3:7D:AA:8F:38:A5:FC:B0:61:FA:D8:D6:B1:A9:F5:6E:0B*

X509SubjectName

Subject CN:	*SUBCA2 MEYSS*
Subject 2.5.4.97:	*VATES-S2819001E*
Subject SERIAL NUMBER:	*S2819001E*
Subject OU:	*PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*
Subject OU:	*S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*
Subject O:	*MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*ci2QPUWGmGyd44n24OQ9d8z9lgI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-05-07T00:00:00Z

19.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

19.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

19.3.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] SUBCA2 MEYSS

Name [es] SUBCA2 MEYSS

Service digital identities

X509SubjectName

Subject CN: SUBCA2 MEYSS

Subject 2.5.4.97: VATES-S2819001E

Subject SERIAL NUMBER: S2819001E

Subject OU: PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

Subject OU: S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

Subject O: MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Subject L: MADRID

Subject C: ES

X509SKI

X509 SK I ci2QPUWGmGyd44n24OQ9d8z9lgI=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2017-04-11T00:00:00Z

19.3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20 - TSP: Consejo General de Colegios Oficiales de Médicos

.

TSP Name

Name	*[en]*	*Consejo General de Colegios Oficiales de Médicos*
Name	*[es]*	*Consejo General de Colegios Oficiales de Médicos de España (CGCOM)*

TSP Trade Name

Name	*[en]*	*Entidad de Certificación de la Organización Médica Colegial (EC-OMC)*
Name	*[es]*	*Entidad de Certificación de la Organización Médica Colegial (EC-OMC)*
Name	*[en]*	*Organizacion Medica Colegial*
Name	*[es]*	*Organizacion Medica Colegial*
Name	*[en]*	*VATES-Q2866017C*
Name	*[en]*	*ORGANIZACION MEDICA COLEGIAL*
Name	*[en]*	*CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS*

PostalAddress

Street Address	*[es]*	*Plaza de las Cortes, 11*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28014*
Country Name	*[es]*	*ES*

PostalAddress

Street Address	*[en]*	*Plaza de las Cortes, 11*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28014*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:certificacion@cgcom.es*
URI	*[en]*	*http://psc.cgcom.es*

TSP Information URI

URI	*[en]*	*http://psc.cgcom.es*
URI	*[es]*	*http://psc.cgcom.es*

20.1 - Service (withdrawn): Qualified Certificates issued by AC EC-OMC

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC EC-OMC*
Name	*[es]*	*Certificados Reconocidos emitidos por AC EC-OMC*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *327575717960763254787111180198092147 8*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFejCCBOOgAwIBAgIQAnbjTGJC0d2UnvKSCWUmhjANBgkqhkiG9w0BAQUFADCBwTELMAkGA1UE
BhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTwwOgYDVQQLEzNDbGFzcyAyIFB1YmxpYyBQ
cmlYXJ5IENlcnRpZmlyYXRpb24gQXV0aG9yaXR5IC0gRzIxOjA4BgNVBAsTMSBjKSAxOTk4IFZl
cmlTaWduLCBJbmMuIC0gRm9yIGF1dGhvcmI6ZWQgdXNlIG9ubHkxHzAdBgNVBAsTFlZlcmlTaWdu
IFRydXN0IE5ldHdvcmswHhcNMDcwMTI2MDAwMDAwWhcNMTcwMTI1MjM1OTU5WjCBvTELMAkGA1UE
BhMCRVMxJTAjBgNVBAoTHE9yZ2FuaXphY2lvbiBNZWRpY2EgQ29sZWdpYWwxHzAdBgNVBAsTFlZl
cmlTaWduIFRydXN0IE5ldHdvcmsxITAfBgNVBAsTGEVudGlkYWQgZGUgQ2VydGlmaWNhY2lvbjE1
MDMGA1UECxMsQ2xhc3MgMiBNYW5hZ2VkIFBLSSBlbmRpdmlkdWFsIFN1YnNjcmlzZXIgQ0ExDDAK
BgNVBAMTA09NQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMb8KxpiaUkZ/v52ldXW
PjsDdpbf7vC/xRSAfxT3WyFIGm8yOSRs3PdpBqBJQadXoBzi0MNuRpCzgtcLaBtYgnQkxVxK2fx
XzBye3DTxRCJpN8o053eNf4bYbJoTzMoSKWnlxj04CQtJqO9WKFqiotG80uCYIs9791VbUlgOFr
fcVXA3tL Info5NE0n5au2bzJhnY0Qn06fcYPzPbPnbszgIIEjh0FK/BJ5yoGAh1fJZ1TnNzmTT8
RH0bl+KZ3hlQ3bCCkhtVFOWlNyY+8T4NYNFVO5ISE1ienhQdw5vv4lhGEXQcaJPSggkf/Vukr+x
nEjglaKqdCaDQAsNuq8CAwEAAaOCAe8wggHrMBIGA1UdEwEB/wQIMAYBAf8CAQAwRAYDVR0gBD0w
OzA5BgighkgBhvhFAQcXAjAqMCgGCCsGAQUFBwIBFhxodHHwczovL3d3dy52ZXJpc2lnbi5jb20v
cnBhMDQGA1UdHwQtMCswKaAnoCWGI2hkdHA6L y9pcmwudmVyaXNpZ24uY29tL3BjYTIzZ1uY3Is
MBEGCWCGSAGG+EIBAQQEAwIBBjAOBgNVHQ8BAf8EBAMCAQYwLAYDVR0RBCUw16QhMB8xHTAbBgNV
BAMTFFByaXZhdGVMYWJlbDQtMjA0OC00MB0GA1UdDgQWBBTTWPzyL7b1vNDcJxk+qxpKYiZdjCB
6AYDVR0jBIHgMIHdoYHHpIHEMIHBMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIElu
YvsPDA6BgNVBAsTM0NvY XNzIDIgLUhVibGlIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBkdXRob3Ip
dHkgLSBHMjE6MDgGA1UECxMxKGMpIDE5OTggVmVyaVNpZ24sIEluYy4gLSBGb3IgYXV0aG9yaXpl
ZCB1c2Ugb25seTEfMB0GA1UECxMWVmVyaVNpZ24gVHJ1c3QgTmV0d29ya4IRA1kvYMyIn6F6Rgm4
W3Bsiq8wDQYJKoZIhvcNAQEFBQADgYEAGyGtnNhiW4gy7ybFhN0VeDgkCQFWxA8Pc0szHAXBlhUHk
hHvw3YV2Vu3145FQhFaS5p+/BDbW4EgMsgV8XgN533+TahFu340xa21e0LITpVSbzl91iYVSbU/QU
wpZ1+LSOzZrLL3gL fjmap0l/4GIbtsfUfZzqSqOAFh8FIgYHD+8M=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer OU: *VeriSign Trust Network*

Issuer OU: *(c) 1998 VeriSign, Inc. - For authorized use only*

Issuer OU: *Class 2 Public Primary Certification Authority - G2*

Issuer O:	*VeriSign, Inc.*
Issuer C:	*US*
Subject CN:	*OMC*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Entidad de Certificacion*
Subject OU:	*VeriSign Trust Network*
Subject O:	*Organizacion Medica Colegial*
Subject C:	*ES*
Valid from:	*Fri Jan 26 01:00:00 CET 2007*
Valid to:	*Thu Jan 26 00:59:59 CET 2017*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:7C:2B:1A:62:69:49:19:FE:FE:76:21:D5:D6:3E:3B:03:76:96:DF:EE:F0:BF:C5:14:80:7F:14:F7:5B:21:48:1A:6F:32:39:24:6C:DC:F7:69:06:A0:49:41:A7:57:A0:1C:E2:D0:C3:6E:46:90:B3:82:D7:0B:68:1B:58:82:74:24:C6:25:71:2B:67:F1:5F:30:72:7B:70:D3:C5:10:89:A4:DF:28:D3:9D:DE:35:FE:1B:61:B2:68:4F:33:28:48:A5:A7:97:18:F4:27:80:BF:42:22:2A:39:62:85:AA:2A:1F:1B:CD:2E:09:87:EC:F7:BF:48:56:15:25:80:E1:6B:7D:C5:57:03:7B:4B:26:79:68:E4:D1:34:9F:96:AE:DA:1C:C9:86:39:D8:D1:09:CE:E9:FA:D8:3E:03:DB:3E:78:6C:CE:02:5F:12:38:74:14:AF:C1:27:7C:A8:18:08:75:7E:36:75:4E:73:73:99:34:FC:44:7D:1B:23:E2:99:DE:19:50:DD:B0:82:92:1B:55:14:E5:A5:20:DC:98:FB:C4:F8:35:83:45:54:EE:65:48:4D:5F:7A:78:50:77:0E:6F:BF:89:61:18:45:D0:71:A2:4F:4A:08:24:7F:F5:6E:92:BF:B1:9C:48:E0:21:A2:AA:74:26:83:40:0B:0D:BA:AF:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.verisign.com/rpa*
CRL Distribution Points	*http://crl.verisign.com/pca2-g2.crl*
Subject Alternative Name	*CN=PrivateLabel4-2048-4*
Subject Key Identifier	*D3:58:FC:F2:2F:B6:F5:BC:D0:DC:27:19:3E:AA:3C:69:29:88:99:76*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*A4:8A:6D:DD:5D:D5:5C:AF:68:CC:AA:E0:A5:98:97:9C:AE:35:BF:D3:AC:6E:20:B5:11:FA:A7:87:4F:BF:B6:92*

Certificate fields details

Version:	*3*
Serial Number:	*350197348691102790538584844277411914 49*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFejCCBOOgAwIBAgIQGlsOO/27Q1i4zixNXsvdGTANBgkqhkiG9w0BAQUFADCBwTELMAkGA1UE
BhMCVVMxF2AVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTwwOgYDVQQLEzNDb2FzcyAyIFB1YmxpYyBQ
cmlYXJ5IENlcnRpZmlpYXRpb24gQXV0aG9yaXR5IC0gRzIxOjA4BgNVBAsTMShjKSAxOTk4IFZl
cmlTaWduLCBJbmMuIC0gRm9yIGF1dGhvcml6ZWQgdXNlIG9ubHkxHzAdBgNVBAsTFlZlcmlTaWdu
IFRydXN0IE5ldHdvcmswHhcNMDcwMTI2MDAwMDAwWhcNMTIwMTI1MjM1OTU5WjCBvTELMAkGA1UE
BhMCRVMxJTAjBgNVBAoTHE9yZ2FuaXphY2hvbiNZWRpY2EgQ29kZWdpYWwxHzAdBgNVBAsTFlZl
cmlTaWduIFRydXN0IE5ldHdvcmsxITAfBgNVBAsTGEVudGlkYWQgZGUgQ2VydGlmaWNhY2lvbjE1
MDMGA1UECxMsQ2xhc3MgMiBNYW5hZ2VkIFBlSSBJbmRpdmlkdWFsIFN1YnNjcmlzZXIgQ0ExDDAK
BgNVBAMTA09NQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMh8KxpiaUkZ/v52ldXW
PjsDdpbl7vC/xRSAfxT3WyF1Gm8yOSRs3PdpBqBJQadXoBz0MNuRpC2gtcLaBtYgnQkxVxK2fx
XzBycS1DYzRCJpNk6053eN6ibYbJoTzMoSKWnhyi0J4C/Q0ycOWKFqioIG80uCYb979lVbUlgtOFr
fcVXA3tLJnlo5NE0n5au2hzJhjnY0QnO6frYPgPbPnhszgJlEjb0FK/BJ3yoGAh1fjZ1TnNzmTT8
RH0bl+KZ3hlQ3bCCkhtVFOWIlNyY+8T4NYNFVO5ISE1fenhQdw5vv4lhGEXQcaJPSggkf/Vukr+x
nEjgJaKqdC'aDQAsNuq8CAwEAAaOCAe8wggHrMBIGA1UdEwEB/wQIMAYBAf8CAQAwRAYDVR0gBD0w
OzA5BgtghkgBhvhFAQcXAjAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20v
cnBhMDQGA1UdHwQtMCswKaAnoCWGI2h0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTIzZzIuY3Js
MBEGCWCGSAGG+EIBAQQEAwIBBjAOBgNVHQ8BAf8EBAMCAQYwLAYDVR0RBCUwI6QhMB8xHTAbBgNV
BAMTFFByaXZhdGVMYWJlbDQtMjA0OC0tMB0GA1UdDgQWBBT7WPzyL7b1vNDcfxk+qtxpKYiZdjCB
6AYDVR0jBIHgMIHdoYHHpHHEMIHBMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIElu
Yy4xPDA6BgNVBAsTM0NsYXNzIDIgU1VibGljIFByaWlhcnkgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkgLSBHMjE6MDgGA1UECxMxKGMpIDE5OTggVmVyaVNpZ24sIEluYy4gLSBGb3IgYXV0aG9yaXpl
ZCB1c2Ugb25seTEfMB0GA1UECxMWVmVyaVNpZ24gVHJ1c3QgTmV0d29ya4IRA1kvYMyIn6F6Rgm4
W3Buq8wIQYJKoZIhvcNAQEFBQADgYEAhoiDkpMjL6M4aAT2k7fIyIajek0DNAlgTwZ7CDpKCB9T
SGUhBVentGVhSWn5NtlF1aSTEf6lMbL/4ENsQz269mp55SDYLHu+Ie3T7uvYufggaUozh6q0WXbVb
Qf7B0hEZdb43xDBmb5Zr0dp80cZjKdNS4VEZcEnyMdZIp0lddDSA=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer OU: *VeriSign Trust Network*

Issuer OU: *(c) 1998 VeriSign, Inc. - For authorized use only*

Issuer OU: *Class 2 Public Primary Certification Authority - G2*

Issuer O: *VeriSign, Inc.*

Issuer C: *US*

Subject CN: *OMC*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Entidad de Certificacion*

Subject OU: *VeriSign Trust Network*

Subject O: *Organizacion Medica Colegial*

Subject C: *ES*

Valid from: *Fri Jan 26 01:00:00 CET 2007*

Valid to: *Thu Jan 26 00:59:59 CET 2012*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:7C:2B:1A:62:69:49:19:FE:FE:76:21:D5:D6:3E:3B:03:76:96:DF:EE:F0:BF:C5:14:80:7F:14:F7:5B:21:48:1A:6F:32
:39:24:6C:DC:F7:69:06:A0:49:41:A7:57:A0:1C:E2:D0:C3:6E:46:90:B3:82:D7:0B:68:1B:58:82:74:24:C6:25:71:2B:67:F1:5F:30:72:7B:70:D3:C5:10:89:A4:DF:28:D3:9D:DE:35:FE:1B:61:B2:68:4F:33:28:48:A5:A7:97:18:F4:
27:80:BF:42:22:2A:39:62:85:AA:2A:1F:1B:CD:2E:09:87:EC:F7:BF:48:56:15:25:80:E1:6B:7D:C5:57:03:7B:4B:26:79:68:E4:D1:34:9F:96:AE:DA:1C:C9:86:39:D8:D1:09:CE:E9:FA:D8:3E:03:DB:3E:78:6C:CE:02:5F:12:38:7
4:14:AE:C1:27:7C:A8:18:08:75:7E:36:75:4E:73:73:99:34:FC:44:7D:1B:23:E2:99:DE:19:50:DD:B0:82:92:1B:55:14:E5:A5:20:DC:98:FB:C4:F8:35:83:45:54:EE:65:48:4D:5F:7A:78:50:77:0E:6F:BF:89:61:18:45:D0:71:A2:4F:
4A:08:24:7F:F5:6E:92:BF:B1:9C:48:E0:21:A2:AA:74:26:83:40:0B:0D:BA:AF:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.verisign.com/rpa

CRL Distribution Points *http://crl.verisign.com/pca2-g2.crl*

Subject Alternative Name *CN=PrivateLabel4-2048-4*

Subject Key Identifier *D3:58:FC:F2:2F:B6:F5:BC:D0:DC:27:19:3E:AA:3C:69:29:88:99:76*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6B:15:6A:E6:9A:C3:76:29:C4:4B:A2:66:57:AE:ED:3B:7D:FE:E9:5F:F3:61:51:6D:97:55:A9:55:6B:CE:4F:52*

X509SubjectName

Subject CN: *OMC*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Entidad de Certificacion*

Subject OU: *VeriSign Trust Network*

Subject O: *Organizacion Medica Colegial*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2018-07-16T00:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

20.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.5*

20.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC EC-OMC*
Name	*[es]*	*Certificados Reconocidos emitidos por AC EC-OMC*

Service digital identities

X509SubjectName

Subject CN:	*OMC*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Entidad de Certificacion*
Subject OU:	*VeriSign Trust Network*
Subject O:	*Organizacion Medica Colegial*
Subject C:	*ES*

X509SKI

X509 SK I	*01j88i+29bzQ3CcZPqo8aSmImXY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

20.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.5*

20.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.1.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC EC-OMC*
Name	*[es]*	*Certificados Reconocidos emitidos por AC EC-OMC*

Service digital identities

X509SubjectName

Subject CN:	*OMC*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Entidad de Certificacion*
Subject OU:	*VeriSign Trust Network*
Subject O:	*Organizacion Medica Colegial*
Subject C:	*ES*

X509SKI

X509 SK I	*01j88i+29bzQ3CcZPqo8aSmImXY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2016-03-31T22:00:00Z*

20.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.5*

20.1.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC EC-OMC*
Name	*[es]*	*Certificados Reconocidos emitidos por AC EC-OMC*

Service digital identities

X509SubjectName

Subject CN:	*OMC*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Entidad de Certificacion*
Subject OU:	*VeriSign Trust Network*
Subject O:	*Organizacion Medica Colegial*
Subject C:	*ES*

X509SKI

X509 SK I	*01j88i+29bzQ3CcZPqo8aSmImXY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-01-27T00:00:00Z*

20.1.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.5*

20.2 - Service (withdrawn): Qualified Certificates issued by AC OMC (new CA)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by AC OMC (new CA)*

Name *[es]* *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *484251359877222014*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIII97CCBt2gAwIBAgIIBrhoC897Tn4wDQYJKoZIhvcNAQEFBQAwgaoxCzAJBgNVBAYTAkVTMRsw
GQYDVQQKEx1BQyBDYW1lcmZpcm1hIFMuQS4xEjAQBgNVBAUTCUE4MjcwMzI4NzFLMEkGA1UEBxNC
TWFkcmlkIChzZWUgY3VycmVudCBhZGRyZXNzIGFlOlGbbdHBzOi8vd3d3LmNhbWVyZmlybWEuY29t
L2FkZHJlc3MpMR0wGwYDVQQDExRBQyBDYW1lcmZpcm1hIC0gMjAwOTAeFw0xNDExMjQxMTA3NTVa
Fw0yNDExMjExMTA3NTVaMGUxCzAJBgNVBAYTAkVTMSUwIwYDVQQKDBxPUkdBTklaQUNJT04gTUVE
SUNBIENPTEVHSUFMMSEwHwYDVQQLDBhFTlRJREFEIERFIENFUlRJRkIDQUNJT04xDDAKBgNVBAMM
A09NQzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALRbioOD0Dw7bgIN2yPMUoQgM
wJwGqAvMMbwEv8DGHW1mYOJEvxSLqub0lZSocUkh1o+swiBlATGXsuq1995MDoRhbR9IlyPx09FU
BFXWySSsrOjpSDiMGMmaz3vB1oa0+t4kkdcHj+Xb7rq0XNvWpklvZxbt/ng7UjKvkgPbSOEO0BA3
L0KwUQVlRjogxRvVFR15/X/GVpEVOwcLcb7qVI/W5gzMF2cnXNEXwJuwPhg3Wlbk6VLppDLKrhI
QuqOefgCGxGBXYHWGnTNi0IfpHcxHHbvvBSzZLdQA5HtNHNZI9bGXjGoUotTN5dEhPDnQ91NiGUz
hdY13NFKL3BGOSgBCZQayTZTIgz1MQsEjNS2MOYhxUuVYalXeQnL+vvuTGIB3Ki+/X2KtNo4AI5
yM2+n73da6tP9G7koT7fQBQRgZ3CRoNasMgb0QwGVzNCS5y1g2BUPBQVDN+JV/JyeN9DCrYbm68k
fufOYtyj2rp/dRgYANF6SlGZwRumKjqZ7QuZDRJjEorcGABHVuiAwy3jgfPoYaIQ92rT+vbkpon
zE8SdBXVoToWXS1JWxoJMxRuc2+KZhLOcHBuZCiTMSmPZcldtdr+QFvAJRc3XXOyIf9j4arKVx
kXsE2RrfaN4HF8hE5yOvgskgZEMPYQEtpsm6JQv4EZ8lu6HAgMBAAGjggNhMIIDXTASBgNVHRMB
Af8ECDAGAQH/AgEAMB0GA1UdDgQWBBTnZBVkvqc1vvc6Ts8tPgcL114/KzCB2QYDVR0jBIHRMIHO
gBTJAA8xIL8n9s7ZC4yuW4ucfNleaGBsqSBrzCBrDELMAkGA1UEBhMCRVUxQzBBBgNVBAcTOk1h
ZiIJpZCAoc2VlIGNlcnlfbnQgYWRkcmVzcyBhdCB3d3cuY2FtZCJmaXJtYS5jb20vYWRkcmVzcyks
EjAQBgNVBAUTCUE4MjcwMzI4NzEbMBkGA1UEChMSQUMgQ2FtZXJmaXJtYSBTLkEuMScwJQYDVQQD
Ex5HbG9tYWwgQ2hhbWlcnNpZ24gUm9vdCAtIDIwMDkCAQIwegYIKwYBBQUHAQEEbjBsMEIGCCsG
AQUFBzAChjZodHRwOi8vd3d3LmNhbWVyZmlybWEuY29tL2NlcnRzL2FjX2NhbWVyZmlybWEtMjAw
OS5jcnQwJgYIKwYBBQUFMAGGGmh0dHA6L y9vY3NuLmNhbWVyZmlybWEuY29tMA4GA1UdDwEB/wQE
AwIBBjAnBgNVHSUEIDAeBggrBgEFBQcDAgYIKwYBBQUHAwQGCCsGAQUFBwMJMD4GA1UdIAQ3MDUw
MwYEVR0gADArMCkGCCsGAQUFBwIBFhJodHRwczovL3BvbGljeS5jYW1lcmZpcm1hLmNvbTB6BgNV
HR8EczBxMDagNKAyhjBodHRwOi8vY3JsLmNhbWVyZmlybWEuY29tL2FjX2NhbWVyZmlybWEtMjAw
OS5jcmwwNbAJoDOGMWhldHA6Ly9jcmwxLmNhbWVyZmlybWEuY29tL2FjX2NhbWVyZmlybWEtMjAw
OS5jcmwwgdoGA1UdESB0jCBs4EWY2VydGlmaWNhY2ltbkBjZNvbSSlcSBtDCBsTELMAkGA1UE
BhMCRVMxDzANBgNVBAgTBk1BRFJJRDEPMA0GA1UEBxMGTUFEUklEMQ4wDAYDVQQREwUyODAxNDEf
MB0GA1UECRMWUExBWkEgREUgTEFTIENPUlRFUyAxMTESMBAGA1UEBRMJUTI4NjYwMTdDMTswOQYD
VQQDFDJDT05TRUpPIEdFTkVSQUwgREUgQ09MRUdlT1MgREUgTcOJREIDT1MgREUgRVNOQcORQTAN
BgkqhkiG9w0BAQUFAAOCAgEAbODURFs76WtpnhbH6y5ezfbWk5TrHqsckgRrqA/UMUEajSxSIHbC
JQ3lz9vzJW/dQHw77RIJBQJvAY3II/s5bRsG+TbEA2f4XL Y1fchU+lYY8suilbEYMnorKlI1uP9y
+aF7OCtLHY1Wt0MYccKwU/tNgrozTwMgPbwCo3e4mTdWgg1Vvu573jFmopi5Agzzcth8ruHmAJp1t
SqZOs8NKExZ9k1tkFiuDtrdFqOUi/4vx9LQKFm9EaaoB1vDAbU5KCyOZrq+dvwpHz9B5EN0995a6
8k/8dmMsAmL4qXr8LV66ugm0HUK7xBwTHIZhi3NzSHvyHJHpmkccUmEbVEjxLrKpJc80bjw2HIQV+
uvUP0jUyLwm+9RV+d4cEQ3Js8WLmUjseHm68gl2lvv0kPDVpUCyUADRkFfnN4YHp54kaNNXlWr1
2hAJ80RDyPY+9DfU9DfGfybtu5Eoe/Cl5jumoU/DuVghRPxpByWp+dNOFJtWCD8I/9QIOmribtK9
mjEZVNm/CqIjwhcl5D737n6QKOEapJVCmDFj2UwxAS9pVR4gqNY9cHkUlfT06yBl+QBc3mZV6JLi
3Lq6L6lBfiR+eWaGD7IkopVYJI+eR/4vUGVH5I5s0WdgIMlvG5avdIGZyTT+ktD3R0wJ/WGAUvxw
cDBSGb+oUmUaBV7igHuZ/ws=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *AC Camerfirma - 2009*

Issuer L: *Madrid (see current address at https://www.camerfirma.com/address)*

Issuer SERIAL NUMBER: *A82743287*

Issuer O: *AC Camerfirma S.A.*

Issuer C: *ES*

Subject CN: *OMC*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject O: *ORGANIZACION MEDICA COLEGIAL*

Subject C: *ES*

Valid from: *Mon Nov 24 12:07:55 CET 2014*

Valid to: *Thu Nov 21 12:07:55 CET 2024*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B4:5B:8A:83:83:D0:3C:3B:6E:09:49:34:9D:B2:3C:C5:28:89:08:0C:C0:9C:06:A8:0B:CC:31:BC:04:BF:C0:C6:1D:6D:
66:60:E2:44:BF:14:8B:AA:E6:F4:95:94:A8:71:49:21:D6:8F:AC:C2:20:65:01:31:97:B2:EA:A5:F7:DE:4C:0E:84:61:6D:1F:5F:97:23:EF:D3:D1:54:04:55:D6:C9:24:AC:AC:E8:E9:48:38:8C:18:C9:9A:CF:7B:C1:D6:86:B4:FA:
DE:24:91:D7:07:8F:E5:DB:EE:BA:B4:5C:DB:D6:A6:49:6F:67:16:ED:FE:78:3B:52:32:AF:92:03:EC:48:E1:0E:D0:10:37:2F:42:B0:51:05:65:46:3A:20:C5:1B:D5:15:1D:79:FD:7F:C6:56:91:15:3B:07:0B:71:BE:EA:54:8F:D6:
E6:0C:CC:17:67:27:5C:D1:17:C0:9B:A2:C0:F8:60:DD:69:5B:93:A5:4B:A6:90:CB:2A:B8:48:41:A8:0E:81:FA:82:1B:11:81:5D:81:D6:1A:74:CD:97:FD:07:A4:77:31:F0:76:EF:BC:1E:73:64:B7:50:03:91:DF:34:73:59:D7:D8:4
6:5E:31:A8:52:8B:53:37:97:44:84:F0:E7:43:DD:4D:88:65:33:85:D6:23:DC:D1:4A:2F:70:46:39:28:01:09:94:1A:C9:36:5F:D6:0C:F5:31:0B:04:8C:D4:B6:30:E6:21:C5:4B:95:61:A9:57:79:09:CB:FA:FB:EE:4C:69:41:DC:A8:A
2:FB:F5:F6:2A:B3:68:E0:07:F9:C8:CD:BE:9F:BD:DD:6B:A7:CF:F4:6E:E4:A1:3E:DF:40:14:11:81:9D:C2:46:83:5A:B0:C8:1B:D1:0C:06:57:33:42:4B:9C:B5:83:60:54:3C:14:15:0C:DF:89:57:F2:72:78:DF:43:0A:B6:1B:9B:A
F:24:7E:E7:CE:62:DC:A3:DA:BA:7F:75:18:18:00:D1:6D:48:91:99:C1:1B:A6:2A:3A:99:ED:0B:99:0D:12:63:12:8A:DC:18:00:47:56:E8:80:C2:FD:E3:81:F3:E8:61:A2:10:F7:6A:ED:4F:EB:DB:92:9A:27:CC:4F:12:74:15:D5:
A1:3A:16:5D:2D:49:5B:1A:09:33:14:5A:7B:6F:8A:66:12:CE:71:F1:DB:69:90:AD:21:33:12:98:F6:6B:25:DB:5D:AF:E4:05:BC:02:51:79:75:D7:3B:29:5F:F6:3E:22:AC:A5:71:91:7B:04:D9:1A:DF:68:DE:07:17:C8:44:E7:23:A
F:82:C9:20:64:43:0F:61:01:2D:A6:C9:BA:22:34:2F:E0:46:7C:96:EE:87:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *E7:64:15:64:BE:A7:35:BE:F7:3A:4E:CF:2D:3E:07:0B:B7:5E:3F:2B*

Authority Key Identifier *C8:00:0F:FC:C6:52:FC:9F:DB:3B:64:2E:32:B9:6E:2E:71:F3:65:79*

Authority Info Access

http://www.camerfirma.com/certs/ac_camerfirma-2009.crt

http://ocsp.camerfirma.com

Extended Key Usage	*id_kp_clientAuth - id_kp_OCSPSigning*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma-2009.crl* *http://crl1.camerfirma.com/ac_camerfirma-2009.crl*
Subject Alternative Name	*certificacion@cgcom.es* *CN=CONSEJO GENERAL DE COLEGIOS DE MÃDICOS DE ESPAÃA, SERIALNUMBER=Q2866017C, STREET=PLAZA DE LAS CORTES 11, OID.2.5.4.17=28014, L=MADRID, ST=MADRID, C=ES*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C1:76:11:DB:7B:31:13:61:E2:0D:7B:82:31:AA:DF:47:8B:CB:7F:FA:0B:E5:85:C0:6D:E2:30:92:23:C2:EF:8A*

X509SubjectName

Subject CN:	*OMC*
Subject OU:	*ENTIDAD DE CERTIFICACION*
Subject O:	*ORGANIZACION MEDICA COLEGIAL*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-01-26T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

20.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.5*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

20.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

20.2.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC OMC (new CA)*
Name	*[es]*	*Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities

X509SubjectName

Subject CN:	*OMC*
Subject OU:	*ENTIDAD DE CERTIFICACION*
Subject O:	*ORGANIZACION MEDICA COLEGIAL*
Subject C:	*ES*

X509SKI

X509 SK I	*52QVZL6nNb73Ok7PLT4HC7dePys=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-07-16T00:00:00Z*

20.2.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.5*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

20.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

20.2.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC OMC (new CA)*
Name	*[es]*	*Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities

X509SubjectName

Subject CN:	*OMC*
Subject OU:	*ENTIDAD DE CERTIFICACION*
Subject O:	*ORGANIZACION MEDICA COLEGIAL*
Subject C:	*ES*

X509SKI

X509 SK I	*52QVZL6nNb73Ok7PLT4HC7dePys=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

20.2.5.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.5*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

20.2.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.2.6 - History instance n.3 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC OMC (new CA)*
Name	*[es]*	*Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities

X509SubjectName

Subject CN:	*OMC*
Subject OU:	*ENTIDAD DE CERTIFICACION*
Subject O:	*ORGANIZACION MEDICA COLEGIAL*
Subject C:	*ES*

X509SKI

X509 SK I	*52QVZL6nNb73Ok7PLT4HC7dePys=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-03-31T22:00:00Z*

20.2.6.6 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.5*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

20.3 - Service (granted): Qualified Certificates issued by CGCOM QUALIFIED 2020

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by CGCOM QUALIFIED 2020*

Name *[es]* *Certificados cualificados emitidos por CGCOM QUALIFIED 2020*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *602469569663099098610212714328505148949152111858*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHvTCCBaWgAwIBAgIUaYerezQJb7VMnfr3U7kdvP8/nPIwDQYJKoZIhvcNAQENBQAwgZ0xCzAJ
BgNVBAYTAkVTMRYwFAYDVQQKDA1Ww61udGVncmlzIFNMMSAwHgYDVQQHDBdIb3NwaXRhbGV0lGR1
IExsb21yZWdhdDEYMBYGA1UEYQwPVAFURVMtQjYyOTEzOTZMSYwJAYDVQQDDB12aW5DQXNpZ24g
UXVhbGlmaWVkIEF1dGhvcml0eTESMBAGA1UECAwJQmFyY2Vsb25hMB4XDTIwMDMwMjEwNDExOFoX
DTMzMDMwMjEwNDExOFowgcYxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIDAZNQURSSUQxDzANBgNVBAcM
Bk1BRFJJRDEYMBYGA1UEYQwPVkFURVMtUTI4NjYwMTdDMSEwHwYDVQQLDBhFTlRJNEFEIERFIENF
UlRJRkIDQUNTI04xOTA3BgNVBAoMMENPTlNFSk8gR0VOR VJBTCBERSBDT0xFR0lPUyBPRkIDSUFM
RVMgREUgTUVESUNPUzEdMBsGA1UEAwwUQ0dDT00gUVVBTElGSUVEIDIwMjAwggIiMA0GCSqGSIb3
DQEBAQUAA4ICDwAwggIKAoICAQCk7vupCucL Uc0SrUtK6xBDLOE39Pk9Myhmnnu/A2YBgroxh08D
3kqv50t+8SAT3K424OrsxjZBMLFpzwHTXY4ZguZe40QJ72azOXqMAL9kymGQRJtZUL6BmCquhN3
SwQrzaBvxIKUC7NwsyqFSMlou5NcXRWERPufmHDrhbhlkfLafcnIeWZ3WgCZZqAwBWqkJw9C3uHch
Ufpy0MNCjyAYBUgS4D2vqcfEL7aXnOoBzVYmLiEP1csJsIJshE9Qj7bAuDmMLV0n7tqb3D7rCS
5Qfj7LzZ1n0U095IXycrOy4Rzy3AFeuqDETt8NI2xbr7M67ss+1E0heANBb0Ad5tCq8MCwiGm14w
0NucjpJjKKUAH7E71FVNrt85+4Sk++d4DvCHx45vzW7NQpt+fbNPJLtunmeGq+shzL/XYlvBcyvQ
Z4DRSxumIU11Fj2Ysv9PsdAbGJNjGpOovvp840MVzKjs8Gm6YIXSshoz4BteRtPfGP6U4ATjxZ
XtwZoUqVt6mxeNQxQyXcCbMGPTTAKWPK2aG8W1+FSOSl4b5P/MyNwt5KctyFkam2mVITRktTs+v
1Kdqkwbq1WNZA/kSeQzJLx/dOp62W0jzyZHwmSn/QEl0PGcnZWximo+ocDLtMuAqFco8vMo0Abvm
FVmnv9w1Ji2/bRKL0L20xAoQzwIDAQABo4IByDCCAcQwHwYDVR0jBBgwFoAU0D5KapJvTbOGR1x0
5FajAvQWyNAwHQYDVR0OBBYEFDJBZJTULUEt6zesrcgmrq42IOtHPMA4GA1UdDwEB/wQEAwIBBjCB
jAYDVR0gBIGEMIGBMH8GBFFdIAAwdzAoBggrBgEFBQcCARYcaHR0cHM6Ly9wb2xpY3kudmlu Y2Fz
aWduLm5ldDBLBggrBgEFBQcCAjA/DD1DZXJ0aWZpY2FkbyBDQSBTdWJvcmRpbmFkYS4gVmVyICBo
dHRwczovL3BvbGljeS52aW5jYXNpZ24ubmV0MB0GA1UdEQQWMBSBEmluZm9AdmluY2FzaWduLm5l
dDBtBgNVHR8EWDBWMCmgI6AIhtNodHRwOi8vY3JsMy52aW5jYXNpZ24ubmV0L2Nhc3ViLmNybDAp
oCegIYYjaHR0cDovL2NybDQudmluY2FzaWduLm5ldC9jYXN1Yi5jcmwwTwYIKwYBBQUHAQEEQzBB
MD8GCCsGAQUFBzAChjNodHRwOi8vd3d3LnZpbmNhc2lnbi5uZXQvcHVibGlja2V5cy9jYXF1YWxp
ZmllZC5jZXIwEgYDVR0TAQH/BAgwBgEB/wIBATANBgkqhkiG9w0BAQ0FAAOCAgEArdL0rqVnO8i9
iZjPs0U4vwfFlaGdpMc5A8hXMAGPCCis8IKS72hur8IxezDcq1Ij9U/z+dFUTCzFmctI6tAsEonf
hl/Qlmk4vzwIfipb1PKFW89mGjxLza2Rq YS9BqS+DdzC1aT/GVTVDvIE6oN6vlczo2aHKKHA7zMJ6
GUQLBYDTGBlZHI1KPVrBpvGk7OYK1vtj/d2JEWnAWIa0CCvlPwhYbnHDAU9k8Zb4mJHPB4vr3PlC
1BOEMr6tAR41YdjqFTZcb14tcLiIBnc1FyAUMLjSOWoDsmmyIZKTPhHidgsKc0bV01u04TrhBuVk
vJ3re0Cq+5MNSDN4RZE+ScMCmnVxC/+hSxOovI3qdXWAylZHAXeEqOarbugsCS2AbfeOjKqZC9xc
tbrE1u7dJlwK/9ojNCzddczzA2YdDJ13XzcMfx7dhYqgPLfopYOOrbg9Izewx1f6dZ0zvdOESEDM9
7i1TRzvC1bgHbDdFcnIUPkCkdEbBZQ0g1gQOs9UtDo1UabggUGC9KbUhu9ObbVs9cx9eRpOOQGs
JvKxqfKTCQ9ax3xq57jdY111thtWKsFKRvN8YDD/vooQke9viTb0q2m5/6Vk9vGfx7d9Gye9Ug/
x/PjSZuIU14OMyAI2dluCuYcDjLG1A/pL0BEw7zMen1gS7ShKDErJtgp86Kd67I=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer ST: *Barcelona*

Issuer CN: *vinCAsign Qualified Authority*

Issuer 2.5.4.97: *VATES-B62913926*

Issuer L: *Hospitalet de Llobregat*

Issuer O: *Víntegris SL*

Issuer C: *ES*

Subject CN: *CGCOM QUALIFIED 2020*

Subject O:	*CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS*
Subject OU:	*ENTIDAD DE CERTIFICACION*
Subject 2.5.4.97:	*VATES-Q2866017C*
Subject L:	*MADRID*
Subject ST:	*MADRID*
Subject C:	*ES*
Valid from:	*Mon Mar 02 11:41:18 CET 2020*
Valid to:	*Wed Mar 02 11:41:18 CET 2033*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A4:EE:FB:A9:0A:E7:0B:51:CD:12:AD:4B:4A:EB:10:43:2C:E1:37:F4:F9:3D:33:28:67:9E:7B:BF:03:66:01:82:BA:31:87:4F:03:DE:4A:AF:E7:4B:7E:F1:20:13:27:72:B8:DB:83:AB:B3:18:D9:04:C2:C5:A7:3C:07:4D:76:38:66:0B:99:7B:8D:10:27:BD:9A:CC:E5:EA:30:02:FD:93:29:86:41:12:62:65:42:FA:06:60:AA:BA:13:77:4B:04:2B:CD:AF:2F:C6:52:94:09:F3:70:B3:2A:85:F0:C2:28:BB:93:6B:5D:15:84:44:FB:9F:98:70:EB:86:1D:24:7C:B6:B4:72:72:1E:59:9D:D6:80:26:59:68:0C:01:5A:AF:09:C3:D1:B7:B8:77:21:51:FA:72:D0:C3:42:8B:20:18:05:48:12:E0:3D:AF:A9:C7:C4:2F:B6:97:9C:EA:01:CD:56:26:2E:21:0F:D5:CB:09:88:97:EC:84:4F:50:FE:3E:DB:02:E0:E6:30:B5:74:9F:BB:6A:6F:70:FB:FE:B0:92:E5:02:23:EC:BC:D9:D6:7D:14:D3:DE:65:5F:27:2B:3B:2E:11:CF:2D:C0:15:EB:AA:0C:44:ED:F0:D7:F6:C5:BA:FB:33:AE:EC:B3:ED:44:D2:17:80:34:16:F4:01:DE:6D:0A:AF:0C:0B:08:86:9B:5E:30:D0:DB:9C:8E:92:63:28:A5:00:1F:B1:3B:D4:55:4D:AE:DF:39:FB:84:A4:FB:E7:78:0E:F0:87:C7:8E:6F:CD:6E:CD:42:9B:7E:7D:B3:4F:24:BB:6E:9E:67:86:AB:EB:21:CC:BF:D7:62:5B:C1:7B:2B:D0:67:80:D1:4B:1B:A6:22:52:75:D4:58:F6:63:1F:4F:FE:C7:40:6C:62:4D:8E:31:A9:3A:8B:EB:A7:CE:34:31:5C:CA:8E:CF:06:9B:A6:25:5D:2B:21:A3:3E:01:B5:E4:5F:3D:F1:8F:E9:4E:00:4E:3C:59:5E:5C:70:66:85:2A:25:5E:A6:C5:E3:50:C5:08:D7:78:26:CC:18:F1:53:02:45:8F:2B:66:86:F1:6D:7E:15:23:92:97:86:F9:3F:F3:32:37:0E:B9:2B:1B:72:16:46:A6:DA:65:48:4D:19:1F:4E:CF:AF:D4:A7:6A:93:06:EA:D5:63:59:03:F9:12:79:0C:C9:2F:1F:DD:3A:9E:B6:5B:48:F3:C9:91:F0:99:29:FF:40:49:74:3C:67:27:65:6C:62:9A:8F:A8:70:32:ED:32:E0:2A:15:CA:3C:BC:CA:34:01:BB:E6:15:59:A7:BF:DC:35:26:2D:BF:6D:12:8B:D0:BD:B4:C4:0A:10:CF:02:03:01:00:01*
Authority Key Identifier	*D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0*
Subject Key Identifier	*32:41:64:94:D4:2D:41:3A:CD:EB:2B:72:09:EB:AB:8D:88:3A:D1:CF*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.vincasign.net* *CPS text: [Certificado CA Subordinada. Ver https://policy.vincasign.net]*
Subject Alternative Name	*info@vincasign.net*
CRL Distribution Points	*http://crl3.vincasign.net/casub.crl* *http://crl4.vincasign.net/casub.crl*
Authority Info Access	*http://www.vincasign.net/publickeys/caqualified.cer*
Basic Constraints	*IsCA: true - Path length: 1*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*6E:8A:B9:A7:28:5D:70:EF:22:FC:7D:23:75:83:8D:65:3B:64:87:48:81:7A:80:63:4B:0C:1A:F1:04:3C:D3:66*

X509SubjectName

Subject CN:	*CGCOM QUALIFIED 2020*
Subject O:	*CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject 2.5.4.97: *VATES-Q2866017C*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *MkFklNQtQTrN6ytyCeurjYg60c8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2020-09-07T01:00:00Z*

20.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

20.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.1.4*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.6*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.12*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.26852.1.1.10.2*

Description

21 - TSP: BANCO DE ESPAÑA

.

TSP Name

Name	[en]	*BANCO DE ESPAÑA*
Name	[es]	*BANCO DE ESPAÑA*

TSP Trade Name

Name	[en]	*BANCO DE ESPAÑA*
Name	[es]	*BANCO DE ESPAÑA*
Name	[en]	*EUROPEAN SYSTEM OF CENTRAL BANKS*
Name	[es]	*EUROPEAN SYSTEM OF CENTRAL BANKS*
Name	[en]	*VATES-V28000024*

PostalAddress

Street Address	[en]	*C/Alcalá, 48*
Locality	[en]	*Madrid*
State Or Province	[en]	*Madrid*
Postal Code	[en]	*28014*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*C/Alcalá, 48*
Locality	[es]	*Madrid*
State Or Province	[es]	*Madrid*
Postal Code	[es]	*28014*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*http://www.bde.es*
URI	[en]	*mailto:escb-pki@pki.escb.eu*

URI	*[en]*	*mailto:pkibde@bde.es*

TSP Information URI

URI	*[en]*	*http://pki.bde.es*
URI	*[es]*	*http://pki.bde.es*
URI	*[en]*	*http://pki.escb.eu*
URI	*[es]*	*http://pki.escb.eu*

21.1 - Service (withdrawn): Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*
Name	*[en]*	*Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *723303645488871776427510793798017000 75*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHHTCCBgWgAwIBAgIQNmpSTaXkSvhBCKFAm5t26zANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQG
EwJFUzEZMBcGA1UECgwQQkFOQ08gREUgRVNQQcORQTEbMB8GA1UEAwwYQkFOQ08gREUgRVNQQcOR
QS1BQyBSQUlaMB4XDTAyMDcyOTA3MDMyOFoXDTE5MDcyOTA3MDMyOFowUjELMAkGA1UEBhMCRVMx
GTAXBgNVBAoMEEJBTkNPIERFIEVTUEHDkUExKDAmBgNVBAMMH0JBTkNPIERFIEVTUEHDkUEtQUMg
Q09SUE9SQVRJVkEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7vJsBDb2wNNlXlINO
TKMOIQz5D69UQOUfksf+bdE1BXz14BKjRyZZusd1hdrdaWz5+TAj/G4j8JR1HILyWKsd8L4osvcS
Jvgel:0VCaT2puGYMnbcw5loVonQoMD9zpag10IAD3sWC10SbQWQs+pWvQ5FitmGgDFTrQnbRS+UF
ztm3bEtkKQ15rv9O4cMph0hf2Szrt8gSem2ISnDw8+uSJ/+FjEYcP4fRwLdCsv1aY/Pr7bVYwSBc
o1nI86dsc2sywYJqSa89wWpfqikQGkYhEQqvq2qSH6DXlnQ1DmlKrhYiHbVssgd2p00H4hxu5SOH
fhrqBIKNvtk+kR23gPFXAgMBAAGjggP0MIID8DASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB
/wQEAwIBBjAdBgNVHQ4EFgQUwkUt9PmS7jNZmOGKCdWaMvNC25cEwgYIGA1UdfwR7MHImAFFdch3Gc
NnOcVhw61Qj48ii49CGTsoU+kTTBLMQswCQYDVQQGEwJFUzEZMBcGA1UECgwQQkFOQ08gREUgRVNQ
QcORQTEbMB8GA1UEAwwYQkFOQ08gREUgRVNQQcORQS1BQyBSQUlaghDxbXWGXXGzPkkGtoXrNmj3i
MIIBBgYDVR0gBIH+MIH7MIH4BgsrBgEEAYGYHAICATCB6DAnBggrBgEFBQcCARYbaHR0cDovL3Br
aSSZG1uZXMvcG9saXRpY2FzMIG8BggrBgEFBQcCAjCBrqBrENlcnRpZmlj YWRvIHN1amV0byBh
OiBEZWNsYXJlb Y2nzbiBkZSBQcuFjdGlj YXMgZGI/gQ2Vyd GlmaWNbY2nzbiBkZWwgQmFuY2GgZGUg
RXNwYfFhLgpAMjAwNCBCYW5jbyBkZSBFc3Bhb8WEuIFRvZG9zIGxvcyBkZXJlY2hvcyByZXNlcnZh
ZG9zICbDL0Fs2Fs4SA0OCwgMjgwMTQgTWFkcmlkLUVzcGHxYSkwLwYIKwYBBQUHAQEEIzAhMB8G
CCsGAQUFBzABhhNodHRwOi8vcGtpdmEuYmRiLmVzMC5cGCysGAQBgZgcAgMGBBwWGkNlcnRpZmlj
YWRvIEFDFNY1Ym9yZGluYWRhMlIBvAYDVR0BIIBszCCAaswgcmgaggcOCgcBsZGFwOi8vLi0NO
PUJBTkNPJTIwREUlMjBFU1BBJUQxQS1BQyUyMFJBSVosQ049U05UEUlMDEsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9QkRF
LERDPUVTP2F1dGhvcml0eVJldm9jYXRpb25MaXN0P2Jhc2U/b2lqZWN0Y2xhc3M9Y1JMRGlzdHJp
YnVtaWtuUG9pbnQwgbcgzbSgzbGGzga5sZGFwOi8vcGlpbGRhcC5iZGUuZXMvQ049Q1JMLENOPUJB
TkNPJTIwREUlMjBFU1BBJUQxQS1BQyUyMFJBSVosQ049SW50ZXJuYXMsQ049UEULENOPUNvbmZp
Z3VyYXRpb24sREM9QkRFLERDPUVTP2F1dGhvcml0eVJldm9jYXRpb25MaXN0P2Jhc2U/b2lqZWN0
Y2xhc3M9Y1JMRGlzdHJpYnVtaW9uUG9pbnQwJ6AIoCOGIWh0dHA6Ly9wa2kuYmRiLmVzL2NybHMv
QUNyYW16LmNybDANBgkqhkiG9w0BAQUFAAOCAQEAEdcSkFia4OJqmujB3Ena7Hzlz6HrumLP4wFa
rRT1WxpTSQBqF5w+j9hwhrG4QF4/2/GfQAtGDcd+T8lQn65ySlPPSC/iMqvfiNxAc/EX0jyYJ11J
RvOZ+k95nUhlQnHx2DC2lFT6pv9jtm8Fkg0FoTk22DpDRPfIXqBPUmOGPdhwIjGzt9j85HZKOAeQ
J8I0ZO5Ov1v/dB5iZO5Da4FHOl0kMKDQcyDz/XiQqVtvmjvoEQFZYWr7eUuxHzOz8j0V2UQX2f5x
+ÿYkYHcLYK/xfoXO5Ont0VYdrxWoP8rwOx8g+ooUFfvbRVsKOTvQsKKTpXie0Lcga5OkDdnSnx5/
VQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *BANCO DE ESPAÑA-AC RAIZ*

Issuer O: *BANCO DE ESPAÑA*

Issuer C: *ES*

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

Valid from: *Thu Jul 29 09:03:28 CEST 2004*

Valid to: *Mon Jul 29 09:03:28 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BB:BC:9B:01:0D:BD:B0:34:D2:17:22:53:4E:4C:A3:0E:7D:0C:F9:0F:AF:54:40:E5:21:92:C1:7E:6D:D1:35:05:7C:F5:E0:12:A3:47:26:59:BA:C7:75:85:DA:DD:69:6C:F9:F9:30:23:FC:6E:23:F0:94:75:1C:82:F2:58:AB:1D:F0:BE:28:B3:F7:92:26:F8:1E:13:FD:15:09:A4:F6:A6:E1:98:32:7E:9E:C3:99:68:56:8B:D0:A0:C0:FD:72:9A:A0:D7:40:2D:0E:3B:16:0B:44:A1:41:64:2C:FA:95:BF:43:91:62:7E:61:A0:0C:54:EB:42:76:D1:4B:E5:05:CE:D9:B7:6C:47:E4:29:0D:79:AE:FF:4E:E1:C3:29:87:48:5F:D9:2C:EB:B7:C8:12:7A:6D:88:4A:70:F0:F3:EB:92:27:FF:85:8C:46:1C:3F:87:D1:C0:B7:42:B2:FD:5A:63:F3:EB:ED:B5:58:C1:20:5E:A3:59:C8:F3:A7:6C:7B:6B:32:C1:82:6A:49:AF:3D:C1:6A:5F:AA:29:10:1A:46:21:11:0A:B2:AB:6A:92:1F:A0:D7:96:74:35:0E:69:4A:AE:16:22:1D:B5:6C:B2:07:76:A7:4D:07:E2:1C:6E:E5:23:87:7E:1A:EA:04:82:8D:BE:D9:3E:91:1D:B7:80:F1:57:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *C2:45:2B:F4:F9:92:EE:33:59:98:E1:82:75:6B:8C:BC:D0:B6:E5:C1*

Authority Key Identifier *57:5E:6F:71:9E:36:73:9C:56:1C:3A:D5:08:F8:F2:2E:3D:08:64:EC*

Certificate Policies

Policy OID: 1.3.6.1.4.1.19484.2.2.1

CPS pointer: http://pki.bde.es/politicas

CPS text: [Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. @2004 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)]

Authority Info Access *http://pkiva.bde.es*

CRL Distribution Points

ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ,CN=SNTPKI01,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ,CN=Internas,CN=PKI,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

http://pki.bde.es/crls/ACraiz.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FF:2C:7C:52:66:D4:84:DB:63:87:C9:9A:0F:EB:F0:60:38:91:76:C4:9D:27:28:79:44:85:85:F1:9F:EC:13:0F*

X509SubjectName

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-07-01T22:00:00Z*

21.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*

Name *[en]* *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

Service digital identities

X509SubjectName

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

X509SKI

X509 SK I *wkUr9PmS7jNZmOGCdWuMvNC25cE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

21.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.1.3 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*
Name	*[en]*	*Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

Service digital identities

X509SubjectName

Subject CN:	*BANCO DE ESPAÑA-AC CORPORATIVA*
Subject O:	*BANCO DE ESPAÑA*
Subject C:	*ES*

X509SKI

X509 SK I	*wkUr9PmS7jNZmOGCdWuMvNC25cE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2015-11-01T00:00:00Z*

21.1.4 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*
Name	*[en]*	*Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

Service digital identities

X509SubjectName

Subject CN:	*BANCO DE ESPAÑA-AC CORPORATIVA*
Subject O:	*BANCO DE ESPAÑA*
Subject C:	*ES*

X509SKI

X509 SK I *wkUr9PmS7jNZmOGCdWuMvNC25cE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-09-26T00:00:00Z*

21.2 - Service (withdrawn): Qualified Certificates issued by ESCB-PKI ONLINE CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by ESCB-PKI ONLINE CA*

Name *[es]* *ESCB-PKI ONLINE CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *585892604051557329053072259594135771 16*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHMTCCBRmgAwIBAgIQLBPhj/21kc5OKVULtaP1nDANBgkqhkiG9w0BAQUFADBTMQswCQYDVQQG
EwJFVTEpMCcGA1UECgwgRVVST1BFQU4gU1ITVEVNIE9GIENFTIRSQUwgQkFOS1MxGTAXBgNVBAMM
EEVTQ0ltUEzIJE7PT1QgQ0EwHhcNMTEwNzIyMTA0NjM1WhcNMjYwNzIyMTA0NjM1WjBVMQswCQYD
VQQGEwJFVTEpMCcGA1UECgwgRVVST1BFQU4gU1ITVEVNIE9GIENFTIRSQUwgQkFOS1MxGzAZBgNV
BAMMEkVTQ0ltUEzIJE9OTEIORSBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANJv
y4ZCs0EnziXahaYZ5gP5o987svHmfC7k+FYJjx1dKUor1mggmNC2F3YSUxc7PaSbxi3GkEyXhiA
+Ip7qcHwEr+KWyr3gZdzhAZIxozFsY5X5O+VjGqU4XbRjDwSO16SPG7fZa3cjzpBDedT0b4ur+L
4+msL+golBskl0/vFHicpzkPw5i3JtfDXlWjwpU8wE3Nli7WBoy97ErbsSsxkDcJ1xcBmEhrJqR
9vXNxPFHJ+HcbNeYgRHLeCX2J1ukx1vKCn1w2EelxFTGkxDR9RjiUpmDBH5g3C8S7N5PGZZ8E8EB
iY+wQvfOSyrM51EYu0JT+V+mFTGnffIv1GSNEYjU4roPXFolozbyCOcQeIV6wUrRBW+F/YmYoAto
TmA/G0XvEz3YT24R6rDeipcK6QqYfILfUYZoLlKE+kUoOOh2GZvmgam9h6xA75Ku5O6aeTXZnD6
zvJCUu5g9RtAfy1kOtqqS+gEiwhvIJHhkVHETIf6rxXpm90CnsXQcevGsV3sblKHYaYxuT0pZ
HgfcZ16lkZX1OlKXk3reMfnzJtkRHUdeDEP0nzLIQdDvp7lvklpMv8UnHFRc+YNiK0bvhF0sWfJ
a99gNR7VscUfIotr/S7KHbH+tD6vmt6fa3eX1nqam2xANQVbO1Q3xQOaST0RqRAMCF2S73G+5AgMB
AAGjggH9MIIB+TAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVH0J4EFgQU5Fne
RCS2pDvDQzcosMikrYtPQMwHwYDVR0jBBgwFoAU/1YUdaWOXKMlZ5tFnB81UvNwCfiowPAYDVR0g
BDUwMzAxBgRVHSAAMCkwJwYIKwYBBQUHAgEWG2h0dHA6Ly9wa2kuZXNjYi5ldS9wb2xpY2llczA/
BggrBgEFBQcBAQQzMDEwLwYIKwYBBQUHMAKGI2h0dHA6Ly9wa2kuZXNjYi5ldS9jZXJ0cy9yb290
Q0EuY3J0MIIBFQYDVR0fBIIBDDCCAQgwggEEoIIBAKCB/YYiaHR0cDovL3BraS5lc2NiLmV1L2Ny
bHMvcm9vdENBLmNvbHaBjmxkYXA6Ly9sZGFwLXBraS5lc2NiLmV1L0NOPUVTQ0ltUEzIJTIwUm9v
dCUyMENBLE9VPVBLSSxPVT1FU0NCLVBLSSxPPUVTQ0lsQz1FVT9jZXJ0aWZpY2F0ZVJldm9jYXRp
b25MaXN0P2Jhc2U/b2lqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGJmh0dHA6Ly9pYW0t
Y3JsLmVzY2luZXUvZXNjY9yb290Q0EuY3Jshh5odHRwOi8vZXNjYnBraS9jcmxzL.3vb3RDQS5j
cmwwDQYJKoZIhvcNAQEFBQADggIBAJ0WCQWK1AosHc0X7pGc1FUsA8o1Bvs13ARcXakyL6f5kqb+
nMV1s7wGJPL8bbVxjlzQX/IAjs6e+dkCELvIteZcMx6RQTQ6g7kqZ3DnjmwR8ZIF8MOXcZqW4P3a
SzwILK3jvssmcmuJc/cFfG/jMx4U9riASg1r2/TVsSFslZem/gwfTqqQUBhNdJhf56oNsByvwSpX
nMOiiN9uLaDChuEugWcv6XTSuhUkyuOCWIm/wRnbDlw9TUqXQ/PNAGulPgZUlbmUU6RBOeoXAXa
B4eGgdG4KMPpwXWfc6P7lwuir+iTkEqeB/4ZqolePNfkKEvspnyfnqEMzEEZUR6fRzhu3
+L1Rb3VKJ/uaARegZ2lcFIMSh7A719vG6g00gU7c/ce1z59ZZ95H9/Z4y2qzmJ9mTZ3GapAY5m
9ABo+b/N4qAGqbKwqFeDF1ITdYQ5AX0i+4UZIUJcd+LOdolmI2yv/PYRjdHTh9KnKTlEg+q9amQ
UvrgtV9KNkZOgzAiZR6rUdKV1zaUZVOe18WgSlwQvTe2lqvachc68lHVaBSo3K8x9ErLhz332xoC
YwztQx9T0GtxSLPY/0MDkqVEug2T6DSojaHvoOi6+L65XvPTC6P1Dcc+6RAa0x4b5jasRMqt7iu5
/CM3ZEutUQuSaLkInZMyRNgQMWRD

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ESCB-PKI ROOT CA*

Issuer O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Issuer C: *EU*

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

Valid from: *Fri Jul 22 12:46:35 CEST 2011*

Valid to: *Wed Jul 22 12:46:35 CEST 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:6F:CB:86:42:B3:41:27:CE:25:DA:85:A6:19:E6:03:F9:A3:DF:3B:B2:F1:E6:7C:2E:E4:F8:56:09:8F:1D:5D:29:4A:2B:D6:68:20:98:D0:A2:D8:5D:D8:49:4C:5E:EC:F6:92:6F:18:B7:1A:41:32:5E:18:80:F8:8A:7B:A9:C1:F0:7F:3F:8A:5B:2A:F7:81:97:73:84:06:48:C6:8C:C5:CD:5E:57:E4:EF:95:8C:6A:94:E1:76:D1:A4:3C:12:3B:5E:92:3C:6E:E5:65:AD:DC:8F:38:C1:0D:E7:53:D1:BE:22:6A:BF:8B:E3:E9:AC:2F:E8:28:94:1B:24:97:4F:EF:14:78:9C:A7:39:0F:C3:98:B7:26:27:C3:5E:55:A3:C2:99:49:F3:01:37:36:58:BB:58:1A:32:F7:B1:2B:6E:C4:AC:C6:40:DC:27:5C:5C:06:61:21:AC:9A:91:F6:F5:CD:C4:F1:47:27:E1:DC:6C:D7:98:81:11:CB:78:25:F6:27:5B:A4:C7:5B:CA:0A:7D:70:D8:47:88:C4:54:C6:93:10:D1:F5:18:E2:52:99:83:04:7E:60:DC:2F:12:EC:DE:4F:19:96:7C:13:C1:01:89:8F:B0:42:F7:CE:4B:2A:CC:E7:51:18:BB:42:53:F9:5F:A6:15:31:A7:7D:FB:6F:D4:64:8D:11:88:D4:E2:BA:0F:5C:5A:25:A3:36:F2:08:E7:10:79:F5:7A:C1:4A:D1:05:6F:85:FD:89:98:A0:0B:68:4E:60:3F:1B:45:EF:13:3D:D8:4F:6E:11:EA:B0:DE:8A:97:0A:E9:0A:98:7D:F2:DF:51:86:68:2E:52:84:FA:45:28:38:E8:76:19:9B:E6:AA:06:A7:F6:1E:B1:03:BE:4A:BB:93:BA:69:E7:D7:66:70:FA:CE:F2:49:09:4B:B9:83:D4:6D:01:FC:B5:90:EB:63:AA:A4:BE:80:48:B0:96:F9:49:8A:12:2C:54:71:13:95:FE:A3:C5:7A:66:F7:40:A7:B1:74:1C:7A:F1:AC:57:7B:1B:94:A1:D8:69:8C:6E:4F:4A:59:1E:07:DE:67:5E:88:91:95:ED:D4:E9:4A:5E:4D:EB:78:C2:27:CC:9B:64:44:75:1D:78:31:0F:D2:7C:CB:95:07:43:BE:9E:C8:BE:49:69:32:FF:14:9C:71:51:73:E6:0D:88:AD:1B:BE:11:74:B1:67:C9:6B:DF:60:35:1E:D5:B1:C5:1F:26:8B:6B:FD:2E:CA:1D:B1:FE:B4:3E:AF:9B:A7:DA:DD:E5:F5:9E:A6:A6:DB:10:0D:41:56:CE:D5:0D:F1:40:E6:92:4F:44:6A:44:03:02:17:64:BB:DC:6F:B9:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *E4:59:DE:44:24:B6:A4:3C:83:43:37:28:B0:C8:A4:AE:26:2D:3D:03*

Authority Key Identifier *D5:85:1D:69:63:97:28:C9:59:E6:D1:67:07:CD:54:BC:DC:02:7E:EA*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://pki.escb.eu/policies

Authority Info Access *http://pki.escb.eu/certs/rootCA.crt*

CRL Distribution Points

http://pki.escb.eu/crls/rootCA.crl

ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20Root%20CA,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint

http://iam-crl.escb.eu/escb/rootCA.crl

http://escbpki/crls/rootCA.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4B:18:76:44:BF:79:4F:83:D0:00:99:9D:79:27:43:3F:75:F3:CF:B1:64:3A:6D:0F:8A:25:94:35:BE:86:1B:7A*

Certificate fields details

Version: *3*

Serial Number: *135646708379632619634537957133020884269*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHMzCCBRugAwIBAgIQZgybEpoKbCFVCTjdVKDtLTANBgkqhkiG9w0BAQsFADBTMQswCQYDVQQG
EwJFVTEpMCcGA1UECgwgRVVST1BFQUAgYCVST1BFQUAgYCVNIE9lIENFTIRSQUwgQkFOS1MxGTAXBgNVBAMM
EEVTQ0ltUEtlIFJPTUQgQ0EwHBgPMjAxMTA3MjIxMDQ2MzVaFw0yNjA3MjIxMDQ2MzVaMFUxCzAJ
BgNVBAYTAkVVMSKwJwYDVQQKDCBFVVJPUEVBTiBTWVNURU0gT0YgQ0VOVFJBTCBCQUSLUzEbMBkG
A1UEAwwSRVNDQi1QS0kgT05MSU5FIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
0m/LhkKzQSfOJdqPphmmA/mj3ay8eZ8Lu14YgmPHVOpSivWaCY0KLYXdhJTF7s9pJvGLeaQTJe
GIDHnpnwIb/P4pbKxcBIbZ8kjGjMXNXfk75WMapThdtGkPBI7Xpl8buVIrdyPOMENS1PRvxIq
v4vj6aw v6CiUGySXT+8UeJynOQ/DmLcmJ8NcVaPCmUnzATc2WLtYGjLJsStuxKzGQNwnXFwGYSGs
mpH29c3E8Ucn4dxs15iBEcl4JfYnW6THW8oKfXDYR4jEVMaTENH1GOJSmYMEfmDcLxLs3k8ZInwT
wQGJ7BC985LKsznURi7QlP5X6YVMad9+2/UZfl0RiNTiug9cWiWjNvIl5xB59XrBStEFb4X9uZig
CZhOYD8bRc8TPdhPbhHqsN6KIwrpCnb98t9RhmguUo/I6RSg46HYZm+aqBqf2HrEDvkq7k7mp59dm
cPrOBkkJS7mD1G0B/LWQ62OqpL6ASLCW+UmKEixUcROV/qPFemb3QKcxdBx6axXexuU/odhpjG5P
SlkeB95nXoiRle3U6UpeTet4wiMm2REdR14MQ/SfMuVB0O+nsi+SWky/xSccVFz5g2IrRu+EXSx
Z8lr32A1HtWxxR8mi2v9Lsodsf60Pq+bp9td5fWcpqbbEA1BVs7VDfA5pJPRGnEAwIXZLvcb7kC
AwEAAaOCAf0wggH5MAKGA1UdfwIBqQfMAMBAf0wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBTk
Wd5EJLakPINDNyiwyKSuJi09AzAfBgNVHSMEGDAWgBTVhR1pY5coyVnm0WcHzVS83AJ+6jA8BgNV
HSAENTAzMDEGBFUdIAAwKTAnBggrBgEFBQcCARYbaHR0cDovL3BraS5lc2NiLmV1L3BvbGiljaWVz
MD8GCCsGAQUFBwEBBDMwMTAvBggrBgEFBQcwAoYjaHR0cDovL3BraS5lc2NiLmV1L2NlcnRzL3Jv
b3RDQS5jcnQwggEVBgNVHR8EggEMMIIBCDCCAQSgggEAoIH9hJoadHRwOi8vcGtpLmVzYZluZXUv
Y3Jscy9yb290QOEuY3JshoGObGRhcDovL2xkYXAtcGtpLmVzY2luZXUvQ049RVNDQi1QS0klMjBS
b290ITIwQ0EsT1U9UEulLE9VPUVTQ0ltUEtlLE89RVNDQixDPUVVP2NlcnRpZmljYXRlUmV2b2Nh
dGlvbkxpc3Q/YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludIYmaHR0cDovL2lh
bS1cmwuZXNjYi5ldS9lc2NiL3Jvb3RDQS5jcmyGHmh0dHA6Ly9lc2NicGtpL2NybHMvcm9vdENB
LmNybDANBgkqhkiG9w0BAQsFAAOCAgEANKj8sGwW5pc+iKwAKrVTTKaAq/8kIrFqt5p+hncEokBn
ivD0PdVz+NycTeufpkaz/Mv7Pldtf2/7pUSNFDIVTauu7nXz2G4c53uHqSatNOCTLw/L9Nx74/uh
9iUTYW3OlON6qnKY0ocyPyIDnwbqVlIS5W0GL5sChEUhIbsU8EduTaEsC9Yo3KfaIn77W9S3UxdF
7bH3I6Fc01wh1ELoG2cIRYvDEMAIhROxKDHgFz9oIZN8MKwzcIqIWjspMzd6JYdpI2U3U+3IFpL
BwWJPtxFcIkZcoRukbgV6cgFS82oqdMc5yc35T36nsg8BYuxZivGMwfinC36HkoSan5KxyFnXcpuF
pndmw5kQNu7hgpkceoEuxVjT14PTWXHdKmTmpl3+9jsKKmTL7OI7Zv37qCcPnOyvfV2y7cOu+kxGZ
R+dJ4Uso7/S/bkZRd+OUo9qW2IRf3Q02tWfZ0EO4qn78soBe6FMS40lRLXoyIDdVsy4Whf33TGoL
B4YLlI5MyjEuXTIe+PgWqQKlt1JMGxm4PSF2rvasBXGeVQmd5XIn4Pj0TTYONJG830ybAMqX/1WR
P2b6F9/sRB793IqLtXQcywF+pU2E36FMwxCYET259d6cm5IyZ7qkHfc2wQIK+qTBbKmw8WZPUKGZ
xz4tRIzXQcBw+KhcoaVEcra6SjC3VVw=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ESCB-PKI ROOT CA*

Issuer O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Issuer C: *EU*

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

Valid from: *Fri Jul 22 12:46:35 CEST 2011*

Valid to: *Wed Jul 22 12:46:35 CEST 2026*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:6F:CB:86:42:B3:41:27:CE:25:DA:85:A6:19:E6:03:F9:A3:DF:3B:B2:F1:E6:7C:2E:E4:F8:56:09:8F:1D:5D:29:4A:2
B:D6:68:20:98:D0:A2:DR:SD:D8:49:4C:5E:EC:F6:92:6F:18:B7:1A:41:32:5E:18:80:F8:8A:7B:A9:C1:F0:7F:3F:8A:5B:2A:F7:81:97:73:84:06:48:C6:8C:C5:CD:5E:57:E4:EF:95:8C6A:94:E1:76:D1:A4:3C:12:3B:5E:92:3C:6E:
E5:65:AD:DC:8F:38:C1:0D:E7:53:D1:BE:22:6A:BF:8B:E3:E9:AC:2F:E8:28:94:1B:24:97:4F:EF:14:78:9C:A7:39:0F:C3:98:B7:26:27:C3:5E:55:A3:C2:99:49:F3:01:37:36:58:BB:58:1A:32:F7:B1:2B:6E:C4:AC:C6:40:DC:27:5
C:5C:06:61:21:AC:9A:91:F6:FS:CD:C4:F1:47:27:E1:DC:6C:D7:98:81:11:CB:78:25:F6:27:5B:A4:C7:5B:CA:0A:7D:70:D8:47:88:C4:54:C6:93:10:D1:F5:18:E2:52:99:83:04:7E:60:DC:2F:12:EC:DE:4F:19:96:7C:13:C1:01:89:
8F:B0:42:F7:CE:4B:2A:CC:E7:51:18:BB:42:53:F9:5F:A6:15:31:A7:7D:FB:6F:D4:64:8D:11:88:D4:E2:BA:0F:5C:5A:25:A3:36:F2:08:E7:10:79:F5:7A:C1:4A:D1:05:6F:85:FD:89:9B:A0:0B:68:4E:60:3F:1B:45:EF:13:3D:D8:4
F:6E:11:EA:B0:DE:8A:97:0A:F9:0A:98:7D:F2:DF:51:86:68:2E:52:84:FA:45:28:38:E8:76:19:9B:E6:AA:06:A7:F6:1E:B1:03:BE:4A:BB:93:BA:69:E7:D7:66:70:FA:CE:F2:49:09:4B:B9:83:D4:6D:01:FC:B5:90:EB:63:AA:A4:
BE:80:48:B0:96:F9:49:8A:12:2C:54:71:13:95:FE:A3:C5:7A:66:F7:40:A7:B1:74:1C:7A:F1:AC:57:7B:1B:94:A1:D8:69:8C:6E:4F:4A:59:1E:07:DE:67:5E:88:91:95:ED:D4:E9:4A:5E:4D:EB:78:C2:27:CC:9B:64:44:75:1D:78:3
1:0F:D2:7C:CB:95:07:43:BE:9E:C8:BE:49:69:32:FF:14:9C:71:51:73:E6:0D:88:AD:1B:BE:11:74:B1:67:C9:6B:DF:60:35:1E:D5:B1:C5:1F:26:8B:6B:FD:2E:CA:1D:B1:FE:B4:3E:AF:9B:A7:DA:DD:E5:F5:9E:A6:A6:DB:10:0
D:41:56:CE:D5:0D:F1:40:E6:92:4F:44:6A:44:03:02:17:64:BB:DC:6F:B9:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *E4:59:DE:44:24:B6:A4:3C:83:43:37:28:B0:C8:A4:AE:26:2D:3D:03*

Authority Key Identifier *D5:85:1D:69:63:97:28:C9:59:E6:D1:67:07:CD:54:BC:DC:02:7E:EA*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://pki.escb.eu/policies

Authority Info Access *http://pki.escb.eu/certs/rootCA.crt*

CRL Distribution Points

http://pki.escb.eu/crls/rootCA.crl

ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20Root%20CA,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint

http://iam-crl.escb.eu/escb/rootCA.crl

http://escbpki/crls/rootCA.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *13:35:26:DC:99:E9:CC:36:62:F8:F5:FA:20:06:30:05:BA:90:E6:63:2B:F3:4F:18:A8:4B:A3:9B:5F:AA:57:00*

X509SubjectName

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2017-07-01T22:00:00Z*

21.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ESCB-PKI ONLINE CA*

Name *[es]* *ESCB-PKI ONLINE CA*

Service digital identities

X509SubjectName

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

X509SKI

X509 SK I *5FneRCS2pDyDQzcosMikriYtPQM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

21.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ESCB-PKI ONLINE CA*

Name *[es]* *ESCB-PKI ONLINE CA*

Service digital identities

X509SubjectName

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

X509SKI

X509 SK I *5FneRCS2pDyDQzcosMikriYtPQM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-02-24T23:00:00Z*

21.3 - Service (withdrawn): Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2*
Name	*[es]*	*Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *330254086257156635579673985528390708 48*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH8jCCBdqgAwIBAgIQGNh2W+aBhsZVR3b1kickgDANBgkqhkiG9w0BAQsFADBOMQswCQYDVQQG
EwJFUzEZMBcGA1UECgwQQkFOQ08gREUgRVNQQcORQTEkMCIGA1UEAwwbQkFOQ08gREUgRVNQQcOR
QS1BQyBSQUIaIFYyMB4XDTE1MDUwNDE2MDAwMFoxXDTMwMDUwNDE2MDAwMFowVTELMAkGA1UEBhMC
RVMxGTAXBgNVBAoMEEJBTkNPIERFIEVTUEHDKUExKzApBgNVBAMMIkJBTkNPIERFIEVTUEHDKUEt
QUMgQ09SUE9SQVRJVkEgVjIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDG1yj4dCU+
+B7TnKu4mT2L1/rH4QAQeDlqheyCR6zD5b4jU34YsRsxrYMJPDzrqtC3Je4cn1kd7Q/1Brx97Lk
J1vYQBWNMrgzoLGkYIRV/y4BBGzSnZcHDQv4IZma3rWc+HWBkZyCJpa7VSmT6Xz7RbfYsdJ/
SKfDcyEcRxnfy3RRmfy6Id7Mp2Dt7SwzkC6vdWu8/NeObtjysmLdIfu0no6NOr6sminnj0UfZSXV
jA8AJsiEIUoIrMbxQpUNNINPLkwOSmCT+IYwbAo8Usj5IGqS8Oqlp3hNDOluukyLlISg32G/x2iZ
g5md87wB2sixSXChFgVcBdpbJbp6HwTW4LpEnsv4JqNkWzpCw+bwhOyvBDuAUtSZ7nK85s0rwFWF
h4XQpWEpMZuOYXjxjCqF3JlF5qOl5MnFcUtOOLtOTC7wQruZhmEiagg0nTEtKgXoh7QPZWDRvdrN
Hce1IrV7MUWlz2ULVaxD+0m3JS3tmvY5FhYoYwaMXJOtac2k9zYHnOQsU5COuJv3gFJvIGc/IS2K
FnZ6ZyHWtHC8vzGvsWwgDiLM7m+Dpd4anH/Vlkamv8XXCrISyTC5ScHydA/fc5AczJrbENtD+mm5
tvd3Uk8HaCYMN9N7zyEDsKylG5IrbCI2BZrKU4cVU/Qse/Gp5ECKOm5IoTJC2gAQbwIDAQABo4IC
wzCCAr8wEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDHt82GA
yEncIsw9DOYo4lxgU91YMIIBBgYDVR0gBIH+MIH7MIH4BgsrBgEEAYGYHAICATCB6DAnBggrBgEF
BQcCARYbaHR0cDovL3BraS5iZGUuZXMvcG9saXRpY2FzMIG8BggrBgEFBQcCAjCBrxqBrENlcnRp
ZmljYWRvIHN1amV0byBhOiBEZWNsYXJlbY2nzbiBkZSBQcuFjdGljYXMgZGUgQ2VydGlmaWNhY2nz
biBkZWwgOmFuY2gzZGUgRXNwYiFhLgpAMjAxNSBCYW5jbyBkZSBFc3Bh8WEuIFRvZG9zIGxvcyBk
ZXJlY2hvcyByZXNlcnZhZG9zICBDL0fSY2Fs4SA0OCwgMgwMTQg1WFkcmlkLUVzcGHxYSkwHwYD
VR0jBBgwFoAUS8zja9NsOTRPTcPeYMIGGZBtbr8wHwYLKwYBBAGBmBwCAwYEEBYaQUMgU3Vib3Jk
aW5hZGEwggEsBgNVHR8EggEjMIIBHzCCARugggEXoIIBE4aBw2xkYXA6Ly8vQ049QkFOQ08lMjBE
RSUyMEVTUEElRDFBLUFDJTIwUkFJWiUyMFYyLENOPVBLSUlERSxDTj1DRFAsQ049UHVibGlpJT1w
S2V5JTIwU2VvdmljZXMsQ049U2VvdmljZXMsQ049QZ9uZmlndXJhdGlvbixEQz1CREUsRENM9RVM/
YXV0aG9yaXR5UmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Q
b2ludIYjaHR0cDovL3BraS5iZGUuZXMvY3Jscy9BQ3JhaXp2Mi5jcmyGJmh0dHA6Ly9wa2kucmVk
YmRILmVzL2NybHMvQUNyYW16djIuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQDGT6HvK5aIwJ9wa5ha
39uxgzTghZlC5JIeUo+zZJIU3gasgFYUgNOH9tp38IUySu3Goof5hgypfyDhJe+zhPV3AzNlbgMa
jHFcVRZgnUVkQfsVw0PNtUAnOmOjZK483P5e8z2ugzrg1+gGdd+xuWnlH8U3ajrIyo5TEARyu9R6
36KVKbYxcs4ICDVuzxjyAXGDyBSOiT5uo5GxxDlYyn0V9HvbLvz3gERbH924m4Obuz7SgPzwuAL9
pCNNNrzH5SnQlR6qCave+tSTM4NpgGm/mxtNYAbsDlbSR4hLuiQ/xdb5BK4ZXeyEX3KdA55bTsk
wDxRa54jDv7Er8wgpwXlISyUSH/aqDsZeqI1Yab992EIFosvxExvLTW98AOYuhteUQf9uC9ql
KYIVvo9wcRG88IadJZ5bPyQWNLTJI1ZI3WWIqcs5Lmhukpaup YBabTiRQ2ptI2fir+4PnsWAcEcCWL
9sn3GNGWb9fF7Ilil15gTJR1OlPwyYzxt6JYCf8L5aZfWWQuxVz5rjINO0VQ1bTP2cp//oirJd7
Vmn4dCkQnVfp9b295h5ADpdjsxLMK5MBxSwo9euY0ptE8aaHF+BhL4PgRwTYhl0lbgu7tNfruQ0B
GP9ZhOwQTkAjKhZjwxFNfEo8WnhKaZEsdTcH7FQ+IRrpwRgV6lGzGqDBdg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *BANCO DE ESPAÑA-AC RAIZ V2*

Issuer O: *BANCO DE ESPAÑA*

Issuer C: *ES*

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA V2*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

Valid from: *Mon May 04 18:00:00 CEST 2015*

Valid to: *Sat May 04 18:00:00 CEST 2030*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C6:D7:28:F8:74:25:3E:F8:1E:D3:9C:AB:B8:99:3D:8B:D7:FA:C7:E1:00:10:78:39:6A:85:EC:82:47:AC:C3:E6:1E:23:
53:7E:18:B1:1B:31:AD:83:09:3C:3C:EB:FE:AB:42:DC:97:B8:72:7D:64:77:B4:3F:D4:1A:F1:F7:B2:E4:27:5B:D8:40:15:8D:32:BA:E0:A0:B1:A4:62:54:55:FF:28:B8:04:6C:ED:4A:DB:D9:78:78:43:43:2E:08:66:66:B7:AD:67:
3E:1D:60:64:67:20:89:A5:AE:ED:55:29:93:E8:96:93:45:B7:D8:B1:F2:7F:48:A7:FF:0D:CC:84:79:1C:67:7F:2D:D1:46:67:F2:E8:97:7B:32:9D:83:B7:B4:B0:CE:40:BA:BD:D5:AE:F3:F3:5E:39:BD:23:CA:C9:8B:74:82:2E:D2:
7A:3A:34:EA:FA:B2:68:A7:8F:45:1F:65:25:D5:8C:0F:00:26:C8:84:21:4A:08:AC:C8:71:42:95:0D:35:F3:4F:2E:4C:0E:4A:60:93:FA:56:30:6C:0A:3C:52:C8:F9:20:6A:92:F0:EA:A5:A7:78:4D:0C:E2:2E:BA:4C:8B:96:54:A0:
DF:61:BF:C7:68:99:83:99:9D:F3:BC:01:DA:C8:B1:49:70:A1:16:05:5C:05:DA:5B:25:BA:7A:1F:04:D6:E0:BA:44:9E:CB:F8:26:A3:64:5B:3A:42:C3:E6:F0:84:EC:AF:04:3B:80:26:D4:99:EE:79:11:E6:CD:2B:C0:55:85:87:85:
D0:A5:61:29:31:9B:8E:61:78:F1:8C:2A:85:DC:91:79:A9:09:79:32:71:5C:52:B9:4E:38:8C:CE:4C:2E:F0:42:BB:99:26:19:84:BA:A8:34:9D:31:1F:90:65:E8:87:B4:0F:65:60:D1:BD:DA:CD:1D:C7:B5:22:B5:7B:31:45:A5:AF:6
5:0B:55:AC:43:FB:49:B7:25:2D:ED:9A:F5:79:16:16:28:63:06:8C:5C:93:B4:69:ED:A4:F7:36:07:9C:E4:2C:53:90:8E:B8:9B:F7:A8:52:6F:20:67:BF:7D:2D:8A:16:76:7A:67:21:D6:B4:70:BC:BF:31:AF:B1:6C:20:0F:22:CC:EE
:6F:83:A5:DE:1A:9C:7F:D5:22:46:A6:BF:C5:D7:0A:B7:D2:C9:30:B9:49:C1:F2:74:0F:DF:7B:90:1C:CC:9A:DB:10:DB:43:FA:69:B9:B6:F7:77:52:4F:07:68:26:0C:37:D3:7B:CF:21:03:B0:AC:A5:1B:92:2B:6C:27:F6:05:9A:C
A:53:87:15:53:F4:2C:7B:F1:A9:E4:40:8A:3A:6E:49:A1:32:42:CE:00:10:6F:02:03:01:00:01
```

Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*31:ED:F3:61:80:C8:49:DC:D6:CC:3D:0C:E6:28:E2:5C:60:53:DD:58*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.19484.2.2.1* *CPS pointer: http://pki.bde.es/politicas* *CPS text: [Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. @2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)]*
Authority Key Identifier	*4B:CC:E3:6B:D3:6C:39:34:4F:4D:C3:DE:60:C2:06:19:90:6D:6E:BF*
CRL Distribution Points	*ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint* *http://pki.bde.es/crls/ACraizv2.crl* *http://pki.redbde.es/crls/ACraizv2.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*64:4B:79:C4:7D:87:C2:9B:31:6A:5C:D7:99:4C:F1:CF:CA:3E:1F:C0:78:55:21:87:56:5F:22:ED:83:25:03:95*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2017-07-01T22:00:00Z*

21.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.3.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2*
Name	*[es]*	*Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

Service digital identities

X509SubjectName

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA V2*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

X509SKI

X509 SK I *Me3zYYDISdzWzD0M5ijiXGBT3Vg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

21.3.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.3.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

Name *[es]* *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

Service digital identities

X509SubjectName

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA V2*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

X509SKI

X509 SK I *Me3zYYDISdzWzD0M5ijiXGBT3Vg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-07-12T22:00:00Z*

22 - TSP: Servicio de Salud de Castilla-La Mancha (SESCAM)

.

TSP Name

Name	*[en]*	*Servicio de Salud de Castilla-La Mancha (SESCAM)*
Name	*[es]*	*Servicio de Salud de Castilla-La Mancha (SESCAM)*

TSP Trade Name

Name	*[en]*	*Servicio de Salud de Castilla-La Mancha (SESCAM)*
Name	*[es]*	*Servicio de Salud de Castilla-La Mancha (SESCAM)*
Name	*[en]*	*JCCM*
Name	*[es]*	*JCCM*
Name	*[en]*	*SESCAM (NIF Q-4500146H)*
Name	*[es]*	*SESCAM (NIF Q-4500146H)*
Name	*[en]*	*VATES-Q4500146H*

PostalAddress

Street Address	*[en]*	*Avenida Río Guadiana*
Locality	*[en]*	*Toledo*
State Or Province	*[en]*	*Toledo*
Postal Code	*[en]*	*45007*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Avenida Río Guadiana*
Locality	*[es]*	*Toledo*
State Or Province	*[es]*	*Toledo*
Postal Code	*[es]*	*45007*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:info_pki@sescam.jccm.es*
URI	*[en]*	*http://www.sescam.jccm.es*

TSP Information URI

URI	*[en]*	*http://sescam.jccm.es/web1/home.do?main=/ciudadanos/avancesMedTecn/cervantes_EN.html*
URI	*[es]*	*http://sescam.jccm.es*

22.1 - Service (withdrawn): Qualified Certificates issued by CA SESCAM CA Entidades Finales

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA SESCAM CA Entidades Finales*
Name	*[es]*	*Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *709074458271001845888313003744295098 23*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFOzCCAyOgAwIBAgIQNVhG/m7nW1VM9Na5WDUovzANBgkqhkiG9w0BAQUFADBWMQswCQYDVQQG
EwJFUzENMAsGA1UECgwESkNDTTEfMB0GA1UECgwWU0VTQ0FNKE5JRiBRLTQ1MDAxNDZJKTEXMBUG
A1UEAwwOU0VTQ0FNIEJvb3QgQ0EwHhcNMTAxMTMwMTA0OTI5WhcNMzUxMTMwMTA0OTI5WjBkMQsw
CQYDVQQGEwJFUzENMAsGA1UECgwESkNDTTEgMB4GA1UECgwXU0VTQ0FNIChOSUYgUS00NTAwMTQ2
SCkxJDAiBgNVBAMMG1NFU0NBTSBDQSBFbnRpZGFkZXMgRmluYWxlczCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANl+n1uXoRRZzahtPyvy2Qvi9wQ4zrUV/FkR07p8HVW11qykzKqLJhKG
oq98EF06s1YajOXXSj5cMU8Yut8q+rBFIKI5/nsp+hgs8vq/OWPlNXOX1Sizel D9WoEKdcXx94fa
9CT0X9CNEj6/mjLDKgf9XxsKq5aQpNcSgt0/r3dfWv9wW/smW2/PVpKhdm62FUk+gsmSXVKTf
63G/ii85u3nLvvHxg0rYcKpGccFx/NQb2QsixSvmqA0sW/Y+whYYTzwhY6GKUUu+xaGWIGZcbt8L
9vUOv8x/WrRJ8EzyA+MQXKPd2KmMbKwshTuPtCb9dKMSWFIYF6Gl9123s4cCAwEAAaOB9jCB8zAS
BgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVH04EFgQUtcO7Xk Tp5C40BOQ3
4x3qUf/fcNB0wHwYDVR0jBBgwFoAUt6BOxzZkVZG2/XccYw7Hb3z9ck0wSQYDVR0gBEIwQDA+BgRV
HSAAMDYwNAYIKwYBBQUHAgEWKGh0dHA6Ly9zZXNjYW0uamNjbS5lcy9wa2kvZHBjL2RwY3YyLmh0
bWwwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL3Nlc2NhbS5qY2NtLmVzL3BraS9jcmxzL3Nlc2Nh
bV9yb290X2NhLmNybDANBgkqhkiG9w0BAQUFAAOCAgEAmyFDvGsYWCk+RWpYgIuQgmAoGhJ1KHBD
gCNBj60DHiwUzI3MuiKd8jnatCbipa9hkRGOrM8+fmWu1voT+AkBu0+5p9oKkj7PpgWQ2guSmCL
YzJXzOo2p9NlSOVwKw3RK7Wf0djR1gkvf4pK9MTVxbuB83k4sEFbfX7jpgtWgQVs9q8QzNbMWIM
uaItvVmP5ykvLz2WmpmCyM8dCDO46Egi0m9IZL/dm6twVXw9zU2Mk273zfITa1iPX4J5TelnZ0Qd
VWT633Wmtrvjiste LjcknHvZkbr/msNvHLcFLWithSitbrFem8JRzd8/Ynt2rMn6S8v7Oy7NVyZyU
T9kr8cuVcvQIu8/Y9yPjIv/tEvt5dcRiaFtmacw+1/yQtaonsIWpoAzS9cc4zYSVFzS98t/FCLzd
Uabl//a+22HyBESRqJ6ayymupKhabag65a0YZQny25TMBwVuLJWwUepPBTsovRcbMM8QQ44dIqukt
lsyxzbRuAU0n4z8z9KFkuoiwVMCoHPZrfyZj+IBO32SJCYO8c11aHbF8PiGbd0tMJhJJ1DiKzbZX
euZ6xpHDmCLn0JUAW4tqvU+LPK9vf/EarY5/ZRWai2bT8O1hgCUU09xSFQdw5VDd90sy9GOPn3n4
fhKtxSgNWT7v1Ew36L C1+wqsjGs4rh5u456esJrC000=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *SESCAM Root CA*

Issuer O: *SESCAM(NIF Q-4500146H)*

Issuer O: *JCCM*

Issuer C: *ES*

Subject CN:	*SESCAM CA Entidades Finales*
Subject O:	*SESCAM (NIF Q-4500146H)*
Subject O:	*JCCM*
Subject C:	*ES*
Valid from:	*Tue Nov 30 11:49:29 CET 2010*
Valid to:	*Fri Nov 30 11:49:29 CET 2035*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D2:3E:9F:5B:97:A1:14:59:CD:A8:6D:3F:2B:F2:D9:0B:E5:F7:04:38:CE:B5:15:FC:59:11:D3:BA:7C:1D:55:B5:D6:AC:A4:CC:AA:8B:26:12:86:A2:AF:7C:10:5D:3A:B1:3C:9A:8C:E5:D7:E6:3E:5C:31:4F:18:B9:FF:2A:FA:B0:45:20:A9:79:FE:7B:29:FA:18:2C:F2:FA:BF:39:63:C8:35:73:97:D7:C8:A2:7A:50:FD:5A:81:0A:75:C5:F1:F7:87:DA:F4:24:F4:5F:D0:8D:10:88:C6:FE:68:CB:0C:A8:A0:7F:D5:F1:B0:AF:EA:E5:A4:29:35:EE:62:83:47:FE:DF:F7:56:F7:05:BF:B2:65:B6:FC:F5:69:2A:17:66:EB:61:54:25:CF:A0:B2:6E:57:54:A4:DF:EB:71:BF:8A:2F:39:BB:79:CB:BE:F1:F1:83:4A:D8:70:AA:46:79:C1:71:FC:D4:1B:D9:0B:22:C5:2B:E6:A8:0D:2C:5B:F6:3E:C2:16:18:4F:3C:21:63:A1:8A:51:4B:BE:C5:A1:96:20:66:5C:6E:DF:0B:F6:F5:0E:BF:CC:7F:5A:B4:49:F0:4C:F2:03:E3:10:5C:A3:DD:D8:A9:8C:6C:AC:2C:85:3B:8F:88:26:FD:74:A3:12:58:52:18:17:A1:A5:F7:5D:B7:B3:87:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*B5:C3:BB:5E:44:E9:E4:2E:34:04:E4:37:E3:1D:EA:51:FA:D2:07:FD*
Authority Key Identifier	*E8:13:AF:C6:26:64:55:91:B6:FD:7C:5C:63:0E:C7:6F:7C:FD:72:4D*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://sescam.jccm.es/pki/dpc/dpcv2.html*
CRL Distribution Points	*http://sescam.jccm.es/pki/crls/sescam_root_ca.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*7B:14:45:2A:70:9D:F3:C6:8C:8E:EB:75:2F:88:78:C0:F5:21:C7:18:8C:23:81:11:DE:1D:DF:82:91:C4:17:2B*

X509SubjectName

Subject CN:	*SESCAM CA Entidades Finales*
Subject O:	*SESCAM (NIF Q-4500146H)*
Subject O:	*JCCM*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-07-01T22:00:00Z

Scheme Service Definition URI

URI [en] *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI [es] *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

22.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA SESCAM CA Entidades Finales*

Name [es] *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales*

Service digital identities

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales*

Subject O: *SESCAM (NIF Q-4500146H)*

Subject O: *JCCM*

Subject C: *ES*

X509SKI

X509 SK I *tcO7XkTp5C40BOQ34x3qUfrSB/0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

22.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.1.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA SESCAM CA Entidades Finales*

Name *[es]* *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales*

Service digital identities

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales*

Subject O: *SESCAM (NIF Q-4500146H)*

Subject O: *JCCM*

Subject C: *ES*

X509SKI

X509 SK I *tcO7XkTp5C40BOQ34x3qUfrSB/0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2012-06-08T00:00:00Z*

22.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.1.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA SESCAM CA Entidades Finales*

Name *[es]* *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales*

Service digital identities

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales*

Subject O: *SESCAM (NIF Q-4500146H)*

Subject O: *JCCM*

Subject C: *ES*

X509SKI

X509 SK I *tcO7XkTp5C40BOQ34x3qUfrSB/0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-09-16T00:00:00Z*

22.1.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.2 - Service (withdrawn): Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012*

Name *[es]* *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *562140996136007997646854501988543782 2*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGhjCCBG6gAwIBAgIQBDqk6M/RhchPS2jUACzDfjANBgkqhkiG9w0BAQUFADBWMQswCQYDVQQG
EwJFUzENMAsGA1UECgwESkNDTTEiMB0GA1UECgwWU0VTQ0FNKE5JRiBRL TQ1MDAxNDZIKTEXMBUG
A1UEAwwOU0VTQ0FNIFJvb3QgQ0EwHhcNMTIwMjI3MTEyODIwWhcNMzcwMjI3MTEyODIwWjBnMQsw
CQYDVQQGEwJFUzEPMA0GA1UECwwGU0VTQ0FNMQ0wCwYDVQQKDARKQ0NNMRIwEAYDVQQFEwlRNDUw
MDE0NkgxJDAiBgNVBAMMG1NFU0NBTSBDQSBFbnRpZGFkZXMgRmluYWxlczCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAKhm1SJkolPtQVBolnCJMSN8qcc3NDxRyIlWSCbuIWqPLdMVF67O
9qr21NnhBiDEojpqkUS4KTieWDFOYnl133mTLBkWcLI+mLxFcFUH/nfoy7P5cU/kLXA+JU1fO4Z0I
JjtnOlf6l/gVzUMDAnBRBaC8DWrIt6lgXY06L2XWdH7BOhHT1eJeqJqWJaw2XvnWHNQfZZQaMX
bTTkNQFaccVAWJvnqhwGQMMMJ4R4pTxlk3fPHO89YvWk7D88xKdaUc+rfvSbPzRywjZH53/dJAK
prp39V8E0bXoyJtjHHaR3iWSBcneNv93NjHtZiXMcrHhnW9RtuJuUaKqNdEJMd8CAwEAAaOCAj0w
ggI5MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSzkpxpSohH
QMSFRtveC9U4KYtVSDAfBgNVHSMEGDAWgBTToIs6/GJmRVkbb9IFxjDsdvfP1yTTCCAVcGA1UdIASC
AU4wggFKMIIBRgYEVR0gADCCATwwNAYIKwYBBQUHAgEWKGhdtHA6Lv9zZXNjYW0uamNjbS5lcy9w
a2kvZHBjL2RwY3YyLmh0bWwwgYQGCCsGAQUFBwICMHgadkxvcyBjZXJ0aWZpY2Fkb3MgZW1pdGlk
b3MgYmFqbyBlc3T1bIHBvbO10aWNhIHNvbiBlbW0aWRvcyBwb3lgZWwgU0VTQ0FNIHBhcmEgQUNz
IHN1Ym9yZGluYWRhcyBkZSBsYSBBQyByYWl6IGRlbCBTRVNDQU0wfQYIKwYBBQUHAgIwcRpvQ2Vy
dGlmaWNhdGVzIGlzc3VlZCBlbmRlciB0aGlzIHBvbGlzeSBhcmUgaXNzdWYkIGUSHRoZSBTRVND
QU0gUm9vdCBDQSB0byBDQXMgc3Vib3JkaW5hdGUgdG8gdGhlIFNFU0NBTSBSb290IENBMDQGCCsG
AQUFBwEBBCgwJjAkBggrBgEFBQcBAYYYaHR0cDovL3Nlc2NhbS5qY2NtLmVzL3ZhMEIGA1UdHwQ7
MDkwN6A1oDOGMWh0dHA6Lv9zZXNjYW0uamNjbS5lcy9wa2kvY3Jscy9zZXNjYW1fcm9vdF9jYS5j
cmwwDQYJKoZIhvcNAQEFBQADggIBAEO6zgnGJCD8bW5WvC4f8zQSFgbON/UPpQtj/w8iQmYBc4s
Xx+TqINseKcp+Q8gzc35R4fUkrFh62BkWrtKq2TL6JQkt0iWSB3+Msn9rB/4RLctmtcj9Ckv4mmx
7EcglNMFQHkRfWMtJHNPH336BCr86AdNzYTYYqSwb3P0sHHtMXdDLJJ4KnbViVMcboZROnUxYL8r
tLfiAS57eH6TNADKaq59bzmkoD5+mLCq5XJHvpZ2O6VL0NgDIcsUbWmv5M5Vy/OCfOnbHvxMEnq
dPR4pcSmR4jN2JRRWukaIbpcmNbvCnf0Sr6GXIdNcsAvJYNh9rm6TCQmns+ZHgLhhNJOAOaCzNK2
//FPjZDO486AKzN2NnYk3o1lZQllpdk5oUYDIJSI14cGqErPbdQZvhh7oHue6hLo13RwgTWStUd
ZgSE61gibx8QELHPk4FD09QG4DrcRhtc+7cv+snntda2HxnG7joNizDMM3o1QevTmUGIsyXdf2zx
LuGgggCJSjpWtMbAB6tzQGjdHKN23WEyuvcMcMi2nPV33W4vEQ87qKtwzSHsDQtTv9GAHaqYPA0M
Y0m+wY6ivdVui/Y/a+dsSywE N5wsZoqUWVPjuVQQjk4E6Sh1h0bnEdlqQner1fh1f6n6vZLteBSZ
wDEjf+tKG4Y2zKcOHU/Frdiiy3j2a

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *SESCAM Root CA*

Issuer O: *SESCAM(NIF Q-4500146H)*

Issuer O: *JCCM*

Issuer C: *ES*

Subject CN: *SESCAM CA Entidades Finales*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: *ES*

Valid from: *Mon Feb 27 12:28:20 CET 2012*

Valid to: *Fri Feb 27 12:28:20 CET 2037*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:66:D5:22:64:A2:53:DF:41:50:68:96:70:89:31:23:7C:A9:C7:B7:34:3C:51:C9:F9:56:48:26:EE:21:6A:8F:2D:D3:15:
17:AE:CE:F6:AA:F6:D4:D9:E1:06:20:C4:A2:3A:6A:91:44:B8:29:38:9E:58:31:4E:62:79:75:DF:79:93:2C:19:16:70:B2:3E:98:BC:45:78:55:07:FE:77:E8:CB:B3:F9:79:49:0B:5C:0F:89:53:57:CE:E1:9D:08:26:3B:67:3A:21:7A:
23:F8:15:CD:43:02:70:51:05:A0:91:0D:6A:C8:8B:A2:20:5D:8D:3A:10:BD:97:59:D1:FB:04:EB:47:4F:57:89:7A:A2:6A:58:96:B0:D9:7B:E7:58:77:CD:40:9D:99:41:A3:17:6C:84:E4:35:01:5A:71:C5:40:58:9B:E7:8E:A8:70
:19:03:0C:30:9E:11:E2:94:F1:96:4D:DF:3C:73:BC:F5:8B:D6:2B:B0:FC:F3:12:9D:69:47:3E:AC:8B:F9:6C:FC:D1:CB:08:D9:1F:9D:FF:76:20:0A:A6:BA:77:F5:5F:04:D1:B5:E8:C8:9B:63:1C:76:91:DE:25:92:05:C9:DE:36:FF
:77:36:31:ED:66:25:CC:72:B1:E1:9D:6F:51:B6:22:6E:51:A2:AA:35:D1:09:31:DF:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *B3:92:9C:69:4A:88:47:40:C4:85:46:DB:DE:19:68:80:29:8B:55:48*

Authority Key Identifier *E8:13:AF:C6:26:64:55:91:B6:FD:7C:5C:63:0E:C7:6F:7C:FD:72:4D*

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://sescam.jccm.es/pki/dpc/dpcv2.html* *CPS text: [Los certificados emitidos bajo está política son emitidos por el SESCAM para ACs subordinadas de la AC raiz del SESCAM]* *CPS text: [Certificates issued under this policy are issued by the SESCAM Root CA to CAs subordinate to the SESCAM Root CA]*
Authority Info Access	*http://sescam.jccm.es/va*
CRL Distribution Points	*http://sescam.jccm.es/pki/crls/sescam_root_ca.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*6F:C2:32:D6:10:27:6E:1B:95:B2:84:8A:E0:B2:60:36:23:C7:80:86:98:C8:97:56:42:AD:40:D2:8F:4B:D2:84*

X509SubjectName

Subject CN:	*SESCAM CA Entidades Finales*
Subject SERIAL NUMBER:	*Q4500146H*
Subject O:	*JCCM*
Subject OU:	*SESCAM*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-07-01T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

22.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012*
Name	*[es]*	*Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012*

Service digital identities

X509SubjectName

Subject CN:	*SESCAM CA Entidades Finales*
Subject SERIAL NUMBER:	*Q4500146H*
Subject O:	*JCCM*
Subject OU:	*SESCAM*
Subject C:	*ES*

X509SKI

X509 SK I	*s5KcaUqIR0DEhUbb3hlogCmLVUg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

22.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.2.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012*
Name	*[es]*	*Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012*

Service digital identities

X509SubjectName

Subject CN:	*SESCAM CA Entidades Finales*
Subject SERIAL NUMBER:	*Q4500146H*
Subject O:	*JCCM*
Subject OU:	*SESCAM*
Subject C:	*ES*

X509SKI

X509 SK I	*s5KcaUqIR0DEhUbb3hlogCmLVUg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2016-06-26T22:00:00Z*

22.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.2.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012*

Name *[es]* *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012*

Service digital identities

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: *ES*

X509SKI

X509 SK I *s5KcaUqIR0DEhUbb3hlogCmLVUg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-06-08T00:00:00Z*

22.2.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.3 - Service (withdrawn): Qualified Certificates issued by CA SESCAM CA Entidades Finales v2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by CA SESCAM CA Entidades Finales v2*

Name *[es]* *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales v2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *147066880981946919780166724887946939210*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGhDCCBGygAwIBAgIQbqQNDcBOEb1WYCOdKFtLSjANBgkqhkiG9w0BAQsFADBZMQswCQYDVQQG
EwJFT1zENMAsGA1UECgwESlNDTTEzMB0GA1UECgwW1J0VTQ0FNKE5IRiBRLTQ1MDAxNDZIKTEaMBgG
A1UEAwwRU0VTQ0FNIE2vb3QgQ0EgdjIwHhcNMTUxMjAzMTExMjI5WhcNNDAxMjAzMTExMjI5WjBq
MQswCQYDVQQGEwJFUzEPMA0GA1UECwwGU0VTQ0FNMQ0wCwYDVQQKDARKQ0NNMRIwEAYDVQQFEwlR
NDUwMDE0NkgxJzAIBgNVBAMMHINFU0NBTSBDQSBFbnRpZGFkZXMgRmluYWxlcyB2MjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBANZrIBLtyjPnh3OnQUKvY0B1A/ZseMc+lDPqno0N1IAO
SVYS8LXcsBbtyaHEFprINHxcTDz7ycLpubCBayNPZYdNnPrPjVMCdBDLVhDpOAOOt1UyoIdT
f525/B8TVIKxJp/Io0NlQo1MyrIlc/gZuOplz1tIZIQAaW7geR5qv60qQyxsH5rK2txpBZNsDPU3
U+LU6y+IAuxNggqWMgksdN9+fpR+Zzldmc86QkRd7Z1ZTUvHBAaL9G+EVrlaOuUdJEo/0pSYg86
18+JHI4AYICWu0+MT4ddNEDJuNzIt1Y0lxn2wrYXLNCkEFPh+ZgkbbOx+FkrytrLjdBLmx8CAwEA
AaOCAjUwggIxMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSJ
6ipENw9MXsy0zhruiaRt6KXFrTAfBgNVHSMEGDAWgBR9pHQvbYsj7aHoZ6KtSW3lc53RgDCCAUwG
A1UdIASCAUMwggEMIIBOwYEVR0gADCCATEwKQYIKwYBBQUHAgEWHWh0dHA6Ly9zZXNjYW0uamNj
bS5lcy9wa2kvZHBjMIGEBggrBgEFBQcCAjB4GnZMb3MgY2VvdGlmaWNhZG9zIGVlaXRpZG9zIGJh
amsgZXN0dSBwb2rtdGlyYSBzfs24gZW1pdGlkb3MgcG9yIGVsIFNFU0NBTSBwYXJhIENfcyBzdWVr
cmRpbmFkYXMgZGUgbGEgQ0EgUmHleiBkZWwgU0VTQ0FNMH0GCCsGAQUFBwICMHEab0NlcnRpZmlj
YXRlcyBpc3N1ZWQgdWSkZXIgdGhpcyBwb2xpY3kgYXJlIGlzc3VlZCBieSB0aGUgU0VTQ0FNIFJv
b3QgQ0EgdG8gQ0FzIHN1Ym9yZGlaYXRlIHRvIHRoZSBTRVNDQU0gUm9vdCBDQTA0BggrBgEFBQcB
AQQaMCYwJAYIKwYBBQUHAQGGGHdoIHA6Ly9zZXNjYW0uamNjbS5lcy92YTBFBgNVHR8EPjA8MDqg
OKA2hjRodHRwOi8vc2VzY2FtLmpjY20uZXMvcGitpL2NybHMvc2VzY2FtX3Jvb3RfY2FfdjluY3Js
MA0GCSqGSIb3DQEBCwUAA4ICAQBuE53xgEkxTAjXaxyTU9nKuUx6J0+LdlgOdagvI2F5sHt7ptlB
QKeXDKPWqo5gAke5LudBFTkGRw6c7PdDo5Zse+7pHh+GTYndAGFqz3tmZLP5vf+xV6t5vFcYpGuS
Q2IKCmBZneKW/HqxcOYaaTxXpem4+ibPTMwick7ak1WS3VCfFWvusYwC4ItUypg/S+c1gaNE3N
zzZGerKIAUbLXqFSG2o6EVvoWuzGqtLQh1/HcFzHjUo7zeN92oHW2F16BVBGZYVaKSFYXomQ
PPkB3z3vzZyUVtO779C8n9laZQLIfZI8iGnDW9vCBqzxd6CXavBdK6dnMMCkk5pSFEbH/idE9LiK
DyMrBDb0GCtseydTGqHf8joKOdXDX+5znchne4MsgmyY+tADIDaUw4xwvblmpM8ksPDdSZCkkpup
Cemc82iLALAKZgdVbaem3jeOCMtO+GT1mSBHi66shEEu0cxJhjP5LFeIONiTWBtaBt/tyyzrnQo0p
eSWKczZMcerWwj/0LRkkXA9zW2qdLMa73Wsdb76pEP7ms/SEdAnIARKONl/xApUjlPLSFzN3RC
UTCU+q6b+6JfE+ul0uAqUy7lN0OVA9i8qQ/oulrz9kwOfuQlJAfcz6+WyzR47usJriicGJf+Cbqy
l4PEgx/wHhta3RnqebWZXdM6Mg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *SESCAM Root CA v2*

Issuer O: *SESCAM(NIF Q-4500146H)*

Issuer O: *JCCM*

Issuer C: *ES*

Subject CN: *SESCAM CA Entidades Finales v2*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: *ES*

Valid from: *Thu Dec 03 12:12:29 CET 2015*

Valid to: *Mon Dec 03 12:12:29 CET 2040*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D6:6B:94:12:ED:CA:33:E7:D3:63:A7:41:42:AF:63:40:F5:03:F6:6C:AC:C7:3E:94:33:EA:9E:8D:0D:D4:80:0E:49:58:
98:F0:B5:DE:E0:18:6D:C9:A7:C7:DC:5A:6B:20:D1:F1:A3:1D:73:4C:3C:FB:C9:E2:E9:BA:10:81:6B:23:4F:65:87:4D:9C:FA:CF:8D:53:02:74:10:CB:56:10:E9:38:03:8E:B7:55:32:A0:87:53:7F:9D:B9:FC:1F:13:54:82:B1:26:9
F:C8:A3:43:48:42:8D:4C:C9:F2:1C:FE:06:6E:42:99:73:D6:D2:19:21:00:1A:5B:BA:9E:47:98:EA:BF:AD:2A:43:2C:6C:1F:9A:CA:DA:DC:69:05:93:6C:0C:F5:37:53:E2:D4:EB:2F:A5:02:EC:4D:AA:0A:96:32:09:2C:74:DF:7E
:96:94:7E:67:39:5D:99:CF:3A:42:44:5D:ED:9D:59:4D:4B:C7:04:06:8B:FF:D1:BE:11:5A:DF:68:EB:94:74:91:28:FF:4A:52:62:0F:3A:D7:CF:89:1C:8E:00:60:80:96:BB:4F:8C:4F:87:5D:34:40:F7:B8:DC:C8:B7:56:34:97:19:F6
:C2:B6:17:2C:D0:A4:10:53:E1:F9:98:24:6D:B3:B1:F8:59:2B:CA:DA:CB:8D:D0:4B:9B:1F:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *89:EA:2A:44:37:0F:4C:5E:CC:B4:CE:1A:EE:89:A4:6D:E8:A5:C5:AD*

Authority Key Identifier *7D:A4:74:2F:6D:8B:23:ED:A1:E8:67:A2:AD:49:6D:E5:73:9D:D1:80*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://sescam.jccm.es/pki/dpc

CPS text: [Los certificados emitidos bajo está política son emitidos por el SESCAM para CAs subordinadas de la CA Raíz del SESCAM]

CPS text: [Certificates issued under this policy are issued by the SESCAM Root CA to CAs subordinate to the SESCAM Root CA]

Authority Info Access *http://sescam.jccm.es/va*

CRL Distribution Points *http://sescam.jccm.es/pki/crls/sescam_root_ca_v2.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CE:9F:E1:F8:BC:D8:9C:47:69:57:C7:82:17:F4:C4:6F:F5:02:2E:B9:06:63:12:36:2F:61:01:6F:62:9E:79:C4*

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales v2*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-07-01T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

22.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA SESCAM CA Entidades Finales v2*
Name	*[es]*	*Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales v2*

Service digital identities

X509SubjectName

Subject CN:	*SESCAM CA Entidades Finales v2*
Subject SERIAL NUMBER:	*Q4500146H*
Subject O:	*JCCM*
Subject OU:	*SESCAM*
Subject C:	*ES*

X509SKI

X509 SK I	*ieoqRDcPTF7MtM4a7omkbeilxa0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

22.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA SESCAM CA Entidades Finales v2*
Name	*[es]*	*Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales v2*

Service digital identities

X509SubjectName

Subject CN:	*SESCAM CA Entidades Finales v2*
Subject SERIAL NUMBER:	*Q4500146H*
Subject O:	*JCCM*
Subject OU:	*SESCAM*
Subject C:	*ES*

X509SKI

X509 SK I	*ieoqRDcPTF7MtM4a7omkbeilxa0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-26T22:00:00Z*

22.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:2.16.724.4.8.10.60.10.3.2.2*

23 - TSP: SIGNE S.A.

.

TSP Name

Name	*[en]*	*SIGNE S.A.*
Name	*[es]*	*SIGNE S.A.*

TSP Trade Name

Name	*[en]*	*SIGNE Autoridad de Certificación*
Name	*[es]*	*SIGNE Autoridad de Certificación*
Name	*[en]*	*VATES-A11029279*

PostalAddress

Street Address	*[es]*	*Avenida de la Industria, 18*
Locality	*[es]*	*Tres Cantos*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28760*
Country Name	*[es]*	*ES*

PostalAddress

Street Address	*[en]*	*Avenida de la Industria, 18*
Locality	*[en]*	*Tres Cantos*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28760*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:signe-ac@signe.com*
URI	*[en]*	*http://www.signe.es/signe-ac*

TSP Information URI

URI	*[en]*	*http://www.signe.es/en*

URI	*[es]*	*http://www.signe.es/signe-ac*

23.1 - Service (withdrawn): Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación*
Name	*[en]*	*Qualified certificates issued by SIGNE- Certification Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2445720188065766261*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHCzCCBPOgAwIBAgIIIfDxjZWpW3UwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1hcHUvZmVzaW9uYWwgQ0lGIEE2
MjYzNDA2ODAeFw0xNTA3MjkxMTIyMjNaFw0zMDEyMzEwNDAyNTVaMIGgMQswCQYDVQQGEwJFUzE9
MDsGA1UEBww0QXZlbmlkYSBkZSBsYSBJbmR1c3RyaWEgMTguIFRyZXMgQ2FudG9zIDI4NzYwLU1h
ZHJpZDETMBEGA1UECgwKU0lIIT1kUjy5BLjESMBAGA1UEBRMJQTExMDI5Mjc5MSkwJwYDVQQDDCBT
SUdORSBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAM2XrSJ0uBB206FoW+I/I9Hb W4VTois+IqlkOZhY5zFqu2SxYH/GLFsI3aVwzbt6XYk/
ukhJgA+W7OunjNOmHDW+0EGauc WdTdHNzguEB6SPmKqMenodGrPWABJpI9Jdy864O+riOqD/6DiZ
YA4HL2+xfoMCESixeNuO67Xw/7Ymcdwqrkcihj1mfQGUUBKbE48yyghrkehDXIvgBeF2COqsMdXsv
YdAxXD13wZqMBkmZIYTYSTxF78lLK3Hs2H1q3nIrI+bzO2tfLTv3C0X9A6ke7Q6mev1bZ9IDxpW2
DPa7om0mdnsgzXSXBQP/Qul/CcGFmxI5Ko8gLq6F9ulP5wUCAwEAAaOCApUwggKRMHQGCCsGAQUF
BwEBBGgwZjA2BggrBgEFBQcwAoYqaHR0cDovL2NybC5maXJtYXByb2Zlc2lvbmFsLmNvbS9jYXJv
b3QuY3J0MCwGCCsGAQUFBzABhBodHRwOi8vb2NzcC5maXJtYXByb2Zlc2lvbmFsLmNvbTAdBgNV
HQ4EFgQUkK0aM71HRW0yREMYbZdkzzuubagwEgYDVR0TAQH/BAgwBgEB wIBADADBgNVHSMEGDAW
gBRlzeurNR4APn7VdMActHNHDhpkLzCCAUEGA1UdIASCATgwggE0MIIBMAYEVR0gADCCASYwgfIG
CCsGAQUFBwICMIHlHoHiAEMAZQByAHQAaQBmAGkAYwBhAGQAbwAgAGQAZQAgAEEAdQB0AG8AcgBp
AGQAYQBkACAAZABlACAAQwBlAHIAdABpAGYAaQBjAGEAYwBpAPMAbgAuACAAQwBvAG4AcwB1AGwA
dABlACAAbABhAHMAIABjAGkAbgBkAGkAYwBpAG8AbgB1AHMAIABkAGUAIAB1AHMAbwAgAGUAbgAg
AGgAdAB0AHAAOgAvAC8AdwB3AHcALgBmAGkAcgBtAGEAcAByAG8AZgBlAHMAaQBvAG4AYQBsAC4A
YwBvAG0ALwBjAHAAczAvBggrBgEFBQcCARYjaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNv
bS9jcHMwOwYDVR0fBDQwMjAwoC6gLIYgaHR0cDovL2NvbC5maXJtYXByb2Zlc2lvbmFsLmNvbS9m
cHUvb3QuY3JsMA4GA1UdDwEB wQEAwIBBjAzBgNVHSUEL DAqBggrBgEFBQcDAgYIKwYBBQUHAwQG
CCsGAQUFBwMJBgorBgEEAYI3FAICMA0GCSqGSIb3DQEBCwUAA4ICAQDJUWwC93tLQPuIAq69DA3k
Nc5JyTmeU9DVCfSosZLI2qH613qVPt8W0PJonEZzWIobLm4QBLnKczTrmCw6pFATL41+Y/c3ZfHp
VFBsXPHkY6zCQszGovsnXKjd2JszzrvMBv9hhdjFasBY7g8elvp0PAnXY5IEaDDEtHlQUCyx4cdS
Mw3vIUvobS4GPcSuH0gt6kpatE7JhikhLig3XbTWxYGpLpe5AIXBfQFF/EUIjgBblCm0IYwOXwd3
k1jPHFNaN5ps4qe6tae18boGANCEXz1fsheXqMAB WPcQqFiugf5L2VXRJsFbjr+L7IbSSR9Im
xLUwQTzmNncrCOWuS4FqGsbcWISC7yPEeyxgK3UsGaSXKPHlsbU2GsA7Vdkwuq7KjWVDa8A6wQ89w
BWcYyz+HPuM+3MHkvGtlUySbMFzyLSjMzMBvvItVYgZJhdn1/7zlA24q3YpZrVlagS9KKVGh8lX
aENhwtePnvOQXFStthmJYxn3EIuJgC/6h3dclhRtUdRQnmyMt73t9vpM8vBGt0DJxR9HUrsKD3h1
Q4yJIAGFJmNNigh1zPW+Ub9YSzHW9g7QIaM1V3fQz8ykFRS2Mw8Lquq9eBuXTlahHZgfG7PXaZ
JP6FQFA4rGrYWgYs2lg0C1AjZMl7YAOAl28O48dqRYs/ishA5k9yiQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *SIGNE Autoridad de Certificacion*

Subject SERIAL NUMBER: *A11029279*

Subject O: *SIGNE S.A.*

Subject L: *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

Subject C: *ES*

Valid from: *Wed Jul 29 13:22:23 CEST 2015*

Valid to: *Tue Dec 31 05:02:55 CET 2030*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:97:AD:27:C9:B8:10:76:D3:A1:68:5B:E2:3F:23:D1:DB:5B:85:53:A2:2B:3E:22:A9:64:39:98:58:E7:31:6A:BB:64:B1:60:7F:C6:2C:5B:08:DD:A5:70:CD:BB:7A:5D:89:3F:BA:48:49:80:0F:96:EC:EB:A7:8C:D3:A6:1C:35:BE:D0:41:9A:B9:E5:9D:4D:D1:CD:CE:0B:84:07:A4:8F:98:AA:8C:7A:7A:1D:1A:B3:D6:00:12:69:23:D2:5D:CB:CE:B8:3B:EA:E2:3A:A0:FF:E8:38:99:60:0E:07:2F:6F:B1:7E:83:02:11:28:B1:78:DB:8E:EB:B5:F0:FF:B6:26:71:DC:2A:AE:47:22:6C:99:9F:40:65:14:04:A6:C4:E3:CC:B2:82:1A:E4:7A:10:D7:7E:F8:01:78:5D:82:3A:AB:0C:75:7B:2F:61:D0:31:5C:3D:77:C1:9A:8C:06:49:99:21:84:D8:49:3C:45:EF:CF:0B:2B:71:EC:D8:7D:6A:DE:72:2B:23:E6:F3:3B:6B:5F:51:3B:F7:0B:45:FD:03:A9:1E:ED:0E:A6:7A:FD:61:67:D2:03:7A:95:B6:0C:F6:BB:A2:6D:26:76:7B:20:CD:74:97:05:03:FF:42:E9:7F:09:C1:85:9B:17:F9:2A:8F:20:2E:AE:85:F6:E9:4F:E7:05:02:03:01:00:01

Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier *90:AD:1A:31:FD:47:45:6D:32:44:43:18:85:97:64:C7:38:AE:6D:A8*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Extended Key Usage *id_kp_clientAuth - id_kp_OCSPSigning - id_kp_smartcardlogon*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1C:B4:70:72:8C:F5:6F:30:20:03:BB:0E:4E:B0:62:41:4F:A1:1D:4F:97:E3:F0:61:17:0C:96:C8:80:71:D7:11*

Certificate fields details

Version: *3*

Serial Number: *3624911463653416953*

X509 Certificate

-----BEGIN CERTIFICATE-----

*MIIGfjCCBGagAwIBAgIIMk5FxUVNn/kwDQYJKoZIhvcNAQELBQAwUTE1MAkGA1UEBhMCRVMxQjBA
BgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1hcHJvZmVzaW9uYWwgQ0lGIEE2
MjYzNDA2ODAeFwOyMDA3MDkxMTE1MDhaFwOzMDEyMzEwNDAyNTVaMIGgMQswCQYDVQQGEwJFUzE9
MDsGA1UEBwwOQXZlbmlkYSBkZSBsYSBJbmR1c3RyaWEgMTgzIFRyZXMgQ2FudG9zID4NcYwU1Uh
ZHJpZDETMBEGA1UECgwKU0lHTkUgUy5BLjESMBAGA1UEBRMJQTExMDI5Mjc5MSkwJwYDVQQDDCBT
SUdORSBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAM2XrSI0uBB206FoW+1/I9Hb W4VTois+IqlkOZhY5zFqu2SxYH/GLFsl3aVwzbt6XYk'
ukhJgA+W7OtnjNOmHDW+0EGaueWdTdHNzguEB6SPmKqMenodGrPWABJp91dy864O+rtOqD/6DiZ
YA4HL2+xfoMCESixeNtO67Xw/7Ymcdwqrkcib1mfQGUUBKbE48yyghrkehDXfvgBeF2COqsMdXsv
YdAxXD13wZqMBkmZIYTYSTxF788LK3Hs2H1q3nIr1+bzO2tfUTv3C0X9A6ke7Q6mev1hZ9IDepW2
DPa7om0mdnsgzXSXBQP/QuUCcGFmxf5Ko8gLq6F9ulP5wUCAwEAAaOCAggwggIEMHQGCCsGAQUF
BwEBBGgwZjA2BggrBgEFBQcwAoYqaHR0cDovL2NvbC5maXJtYXBhb2Zlc2hvbmFsLmNvbS9YXQv
b3Qu Y3J0MCwGCCsGAQUFBzABhBodHRwOhbvb2NzcC5maXJtYXBhb2Zlc2hvbmFsLmNvb1AdBgNV
HQ4EFgQUkK0aMf1HRW0yREMYhZdkxziubagwEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAW
gBRlzeurNR4APn7VdMActHNHDhpkLzCBywYDVR0gBIHDMIHAMIG9BgRVHSAAMIG0MIGABggrBgEF
BQcCAjB0DHJDZXJ0aWZpY2FkbyBkZSBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2nDs24uIENvbnN1
bHRlIGxhcyBjb25kaWNpb25lcyBkZSBlc2BgZW4gaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFs
LmNvbS9jcHMwLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cuZmlybWFwcm9mZXNpb25hbC5jb20vY3Bz
MDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20vZnByb290
LmNvbDAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMA0GCSqG
SIb3DQEBCwUAA4ICAQCztrr6KZDLiFI2B7Tef8b8244LwggHyOqXbAUlRqaNPuqYTLkT2tW+lDXeC
fi7jUAu2nIcizfsI5RR36dykxG8dhrM4GbdofgBePsIXdePDNmn3vyjpaKNiQxODXHknP+No1g24
6LApo0mG8m9MIpCAycplatH9QzdSoAt1NjWbNqS3kxr3xIA5SVJAOWgi36srhsgn2AmGHyLkTQMc
9IRM4rcMeO4o1Iy1hAfpxYywb2Qqhvo TKVYE7oiFx+K7qAqaEG5GwcN4X1i9rqmKGlTqAe/E0fFO
2TGFZIKhcIYarWjNbo4FxNNsworWE9YzuaKh2m1cb6SvKKWYLtOD3ZpgGtGspDseFiSsfo14Khfj
J2ecypiXUHmv5tOq4Mz9JOTLYyl/8xzUxwccPmhpnUlSD80LuazVLIAOOYZYpj/Z9p0j/9YjxlyW
QXsO9saUEtr3Xl7hy8XHoV4CsnlJXz2a0zduNZK2rxp/1Bt7n8IdO3I3CRK1XLq8vNLOz3b78NiP
DuCCP1BkS8ddNaGJo7UyDGCHBqwlnYCYz6I5x7MShsKFl2SNM592Iwn+LxFWP8AJZPDbuqaOXgiP
DAdSv1+VgAdbmD1NjNoJBQ8BTESZAVOzJcAaN5HDsynnitn14VfcZsgNYXjyoQ3bOyl2bF5xyvTE
E53l6z5TX5Ndd7DZRA==*

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Autoridad de Certificacion Firmaprofesional CIF A62634068*
Issuer C:	*ES*
Subject CN:	*SIGNE Autoridad de Certificacion*
Subject SERIAL NUMBER:	*A11029279*
Subject O:	*SIGNE S.A.*
Subject L:	*Avenida de la Industria 18. Tres Cantos 28760-Madrid*
Subject C:	*ES*
Valid from:	*Thu Jul 09 13:15:08 CEST 2020*
Valid to:	*Tue Dec 31 05:02:55 CET 2030*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:97:AD:27:C9:B8:10:76:D3:A1:68:5B:E2:3F:23:D1:DB:5B:85:53:A2:2B:3E:22:A9:64:39:98:58:E7:31:6A:BB:64:B1:60:7F:C6:2C:5B:08:DD:A5:70:CD:BB:7A:5D:89:3F:BA:48:49:80:0F:96:EC:EB:A7:8C:D3:A6:1C:35:BE:D0:41:9A:B9:E5:9D:4D:D1:CD:CE:0B:84:07:A4:8F:98:AA:8C:7A:7A:1D:1A:B3:D6:00:12:69:23:D2:5D:CB:CE:B8:3B:EA:E2:3A:A0:FF:E8:38:99:60:0E:07:2F:6F:B1:7E:83:02:11:28:B1:78:DB:8E:EB:B5:F0:FF:B6:26:71:DC:2A:AE:47:22:6C:99:9F:40:65:14:04:A6:C4:E3:CC:B2:82:1A:E4:7A:10:D7:7E:F8:01:78:5D:82:3A:AB:0C:75:7B:2F:61:D0:31:5C:3D:77:C1:9A:8C:06:49:99:21:84:D8:49:3C:45:EF:CF:0B:2B:71:EC:D8:7D:6A:DE:72:2B:23:E6:F3:3B:6B:5F:51:3B:F7:0B:45:FD:03:A9:1E:ED:0E:A6:7A:FD:61:67:D2:03:7A:95:B6:0C:F6:BB:A2:6D:26:76:7B:20:CD:74:97:05:03:FF:42:E9:7F:09:C1:85:9B:17:F9:2A:8F:20:2E:AE:85:F6:E9:4F:E7:05:02:03:01:00:01*
Authority Info Access	*http://crl.firmaprofesional.com/caroot.crt* *http://ocsp.firmaprofesional.com*
Subject Key Identifier	*90:AD:1A:31:FD:47:45:6D:32:44:43:18:85:97:64:C7:38:AE:6D:A8*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]* *CPS pointer: http://www.firmaprofesional.com/cps*
CRL Distribution Points	*http://crl.firmaprofesional.com/fproot.crl*
Extended Key Usage	*id_kp_clientAuth*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C4:2C:E0:22:D0:A3:45:7B:6B:D6:97:87:11:CE:7B:C7:43:85:C4:B3:4E:11:EB:C8:BA:EE:8B:1D:1B:83:27:99*

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion*

Subject SERIAL NUMBER: *A11029279*

Subject O: *SIGNE S.A.*

Subject L: *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-04-21T00:00:00Z*

23.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.3.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.3.2*

23.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

23.1.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.10.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.5.3

Description

23.1.5 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación

Name [en] Qualified certificates issued by SIGNE- Certification Authority

Service digital identities

X509SubjectName

Subject CN: SIGNE Autoridad de Certificacion

Subject SERIAL NUMBER: A11029279

Subject O: SIGNE S.A.

Subject L: Avenida de la Industria 18. Tres Cantos 28760-Madrid

Subject C: ES

X509SKI

X509 SK I kK0aMf1HRW0yREMYhZdkxziubag=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2019-10-28T01:00:00Z

23.1.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.3.2*

23.1.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.1.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

23.1.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.2.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.10.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.5.3*

Description

23.1.6 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación*
Name	*[en]*	*Qualified certificates issued by SIGNE- Certification Authority*

Service digital identities

X509SubjectName

Subject CN:	*SIGNE Autoridad de Certificacion*
Subject SERIAL NUMBER:	*A11029279*
Subject O:	*SIGNE S.A.*
Subject L:	*Avenida de la Industria 18. Tres Cantos 28760-Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*kK0aMf1HRW0yREMYhZdkxziubag=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-01-16T01:00:00Z*

23.1.6.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.3.2*

23.1.6.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

23.1.6.7 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

23.1.6.8 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.10.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.5.3

Description

23.1.7 - History instance n.3 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación

Name [en] Qualified certificates issued by SIGNE- Certification Authority

Service digital identities

X509SubjectName

Subject CN: SIGNE Autoridad de Certificacion

Subject SERIAL NUMBER:	*A11029279*
Subject O:	*SIGNE S.A.*
Subject L:	*Avenida de la Industria 18. Tres Cantos 28760-Madrid*
Subject C:	*ES*

X509SKI

X509 SK I	*kK0aMf1HRW0yREMYhZdkxziubag=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

23.1.7.9 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.3.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.3.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.10.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.36035.1.10.2*

23.1.7.10 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.1.8 - History instance n.4 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación*

Name *[en]* *Qualified certificates issued by SIGNE- Certification Authority*

Service digital identities

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion*

Subject SERIAL NUMBER: *A11029279*

Subject O: *SIGNE S.A.*

Subject L: *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

Subject C: *ES*

X509SKI

X509 SK I *kK0aMf1HRW0yREMYhZdkxziubag=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-10-07T00:00:00Z*

23.1.8.11 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.3.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.3.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.10.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.10.2*

23.2 - Service (granted): Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020*

Name *[en]* *Qualified Certificates issued by SIGNE Autoridad de Certificación - 2020*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *112294622129710941060350492154332911733*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG8TCCBNmgAwIBAgIQVHsoVDwxEslytvKRXyMYdTANBgkqhkiG9w0BAQsFADBRMQswCQYDVQQG
EwJFUzFCMEAGA1UEAwwSQXV0b3JpZGFkIGRlIENlcnRpZmlyYWNpb24gRmlybWFwcm9mZXNpb25b
bCBDSUYgQTYyNjM0MDY4MB4XDTIwMDczMDA5MjYwNFoXDTMwMTIzMTA0MDI1NVowgZMxCzAJBgNV
BAYTAkVTMRMwEQYDVQQKDApTSUdORSBTLkEuMRgwFgYDVQRhDA9WQVRFUy1BMTEwMjkyNzkzIzAh
BgNVBAsMGkF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uMTAwLgYDVQQDDCdTSUdORSBBdXRvcmlk
YWQgZGUgQ2VydGlmaWNhY2lvbiAtIDIwMjAwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoIC
AQDPyXZgE+AE9SxnXjIlE1ESIRo1ac4xuD9GEzpyj8XsonSvyvdE2y4mjr9SpezJUm1DnQkW
N9MuknbGoBv7os6JyWr5hCL8SrmOE3yiug+Cwd7fCS24AmrTIsAI7WHDcF7lI4VXEfKlLmT152L
qSrxI9jHYnqZeRcwz3Tgjwtt2sUlRd1NSbNDP11L3bg0DE05McZ49EEA4i5EFp8M5JdNdxfPCrGH
v+EyZdKN84Y5qZ4Zfn/luqOyM7V1YOeTq3sJUgJtWVT+8l9tbmKyiTROIBh96kawRrIQOHXqUv1
tFb+oDnWTJRib1+S0SRyY2M311Oqk33n4v1nb4DuURRwZNYTFiuDprGdJ3+cQqGK6EqCLCkXrva/Fy
SshF+Cyb0Zy4aKZPIBjmDij7ws5uhU0sSKXwxKU8tt02rgrsT7RbHmhdur98aPSRTAjRVVYvAAAC
YtKQLgWWs2wc/aZEaefGNA6YIKy4uuSpk9ijsy0DSXWpjUPgVDyEvt2XwMFgFi8Bm3k9HwXRVq6a
gMGpjkhUbOFyJyWld8b2fAK/aOSQ91kVwjmA6XitbuKUkxNDqi3XRycbVTtB46du41dn3cfL5i8
8hkecalBDKRTgWeA+3xsQ7MkrxXpbsJGePbZejo9VspMUirJe6HLxyK3KN1j7GhcDT8Mr3tqcQM
1wIDAQABo4IBgDCCAXwwdAYIKwYBBQUHAQEEaDBmMDYGCCsGAQUFBzAChipodHRwOi8vY3JsLmZp
cm1hcHJvZmVzaW9uYWwuY29tL2Nhcm9vdC5jcnQwLAYIKwYBBQUHMAGGIGh0dHA6Ly9vY3NwLmZp
cm1hcHJvZmVzaW9uYWwuY29tMB0GA1UdDgQWBBQiOoLmqD+p4+ojoKv2jQRLSHtozDASBgNVHRMB
Ai8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFGXN66s1HgA+ftV0wBy0cOGmOyMEQGA1UdIAQ9MDsw
OQYEVR0gADAxMC8GCCsGAQUFBwIBFiNodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Nw
czA7BgNVHR8ENDAyMDCgLqAshipodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Zwcm9v
dC5jcmwwDgYDVR0PAQH/BAQDAgEGMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDANBgkq
hkiG9w0BAQsFAAOCAgEABc2EBUX4WVdXlpqLyMdbwU/+wiOpbEYanb3P5OIFlSb8P6p84yvBLKJ
XIBta02UDt6Dpb8RQHgdIJM7OJOYvFjLPyR1RBDuSbxCA0Rf0fc59U+NQ7xFTnGoqsB9bcxLv4KhX
nJvYJPT2BzEndceAgX+qd3iVJTNJgJGV0gqmD/nqR19uLbY/SzMeyUZIQ6r+vq5Uz4kO00IHZrs1
VXf+VfTLPOSNljxubfuTNdPhUfysWo5N3UskCClb0gtt5+efq7kplprCCorlcMoal2yCCVsNuKUB
7GR4lR1u21s2Mpp98SosWDXXrjDbYtOyCmVNoJiU0jlzzGc1IAnqdpxaWI8rAGoJEA8w146IJKc
uLwUcqidIn3id7SNUMspQQFfinKQIbvcKt5CIP8kjnXc+yVWt+38qQnUMo789NAz2XGIMX5Qt0d
kK/JF2xqZ/qcik++uIji1Y+moxnkWO+rZ3MKNndHSzULE+JFwjp0w67xxHLjpYeuSiFy1J1gi/w
c1/0c7RWdudBTsna2uFR5KD7mm9hRma1mUD575HkvzQF0CSPjfeZ4FW60wXn1IdywF7DJQPzgu2q
e+ILDrq+KQ3q4IRlevUF+rzfg1c/tjNQ1IzvxUthnujATYi+f3/urkX9EJRBPnSHiGwHtxhdwhVX
864IbIQkc1x2KCqOoIQ=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *SIGNE Autoridad de Certificacion - 2020*

Subject OU: *Autoridad de Certificacion*

Subject 2.5.4.97: *VATES-A11029279*

Subject O: *SIGNE S.A.*

Subject C: *ES*

Valid from: *Thu Jul 30 11:26:04 CEST 2020*

Valid to: *Tue Dec 31 05:02:55 CET 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CF:FF:2F:19:A4:4F:80:93:D4:B1:99:78:E5:94:4D:44:E6:52:11:A3:5B:1C:E3:1B:83:F4:61:33:A7:28:FC:5E:CA:32:4A:F8:AF:E0:4D:B2:E2:68:E2:F5:2A:5E:78:9F:C9:52:6D:43:9D:09:16:37:D3:2E:92:76:C6:A0:1B:FB:A2:CE:89:C9:6A:F9:84:22:FC:4A:B9:8E:13:7B:E3:BA:0F:82:73:07:7B:7C:24:B6:E0:09:AB:4C:8B:00:23:B5:87:0D:C1:7B:94:8E:15:5C:47:CA:94:B9:93:23:9D:8B:A9:2A:F1:23:D8:C7:62:7A:99:79:17:30:CF:74:E0:8F:0B:6D:DA:C5:25:45:DD:4D:49:B3:43:3F:5D:4B:DD:B8:34:0C:4D:39:31:C6:78:F4:41:00:E2:2E:44:16:9F:0C:E4:97:4D:77:17:CF:0A:B1:87:BF:E1:32:65:D2:8D:F3:86:39:A9:9E:19:7E:7F:C8:8A:A3:B2:33:B5:75:60:E7:93:AB:7B:23:52:08:C8:B5:65:48:FB:C9:7D:B5:B9:8A:CA:24:D1:38:80:61:F6:89:1A:C1:1A:E5:40:E1:D7:A9:4B:E5:B4:56:FE:A0:39:D6:4C:94:62:6F:5F:92:D1:24:63:63:63:37:D4:83:AA:93:7D:E7:E2:FD:67:6F:80:DA:51:14:70:64:D6:13:16:2B:83:A4:67:49:DF:E7:90:A8:62:BA:12:A0:8B:91:7A:EF:6B:F1:72:4A:C8:45:F8:2C:9B:D1:9C:B8:68:A6:4F:20:18:E6:0E:28:FB:C2:CE:6E:84:ED:2C:48:A5:F0:C4:A8:89:F2:7D:36:AE:0A:EC:4F:B4:5B:1E:68:5D:9E:DF:7C:68:F4:91:4C:08:D1:55:56:2F:00:00:02:62:D2:90:2E:05:96:B3:6C:1C:FD:A6:44:69:E7:C6:34:0E:98:20:AC:B8:BA:E4:A9:93:D8:A3:B3:2D:03:49:75:A9:8D:43:E0:54:3C:84:BE:DD:97:C0:C1:60:16:2F:01:9B:79:3D:1F:05:D1:56:AE:9A:80:C1:A9:8E:48:48:25:B3:85:C8:8C:96:95:DF:1B:D9:F0:0A:FD:A3:92:43:DD:64:57:08:E6:03:A5:E2:B5:BB:8A:52:4C:4D:0E:A8:B7:5D:1C:9E:6D:54:ED:07:8E:9D:BB:8D:5D:9F:77:1F:2F:98:BC:F2:19:1E:71:A9:41:0C:A4:53:A9:67:80:FB:7C:6C:43:B3:24:AE:25:E9:6E:C2:46:78:F6:D9:7A:3A:3D:56:CA:4C:52:2A:C9:7B:A1:CB:C7:22:B7:28:DD:63:EC:68:5C:0D:3F:0C:AE:2D:ED:A9:C4:0C:D7:02:03:01:00:01

Authority Info Access

http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier *22:3A:82:E6:A8:3F:A9:E3:EA:23:A0:AB:F6:8D:04:4B:48:7B:68:CC*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Extended Key Usage *id_kp_clientAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B8:DF:38:4F:1F:CD:6E:CB:3F:4D:7D:D6:38:0E:54:D3:54:C6:12:56:56:0A:59:9D:80:45:32:47:D9:3A:F5:EA*

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion - 2020*

Subject OU: *Autoridad de Certificacion*

Subject 2.5.4.97: *VATES-A11029279*

Subject O: *SIGNE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *IjqC5qg/qePqI6Cr9o0ES0h7aMw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

23.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

23.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.2.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.10.3*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.36035.1.5.3*

Description

24 - TSP: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

.

TSP Name

Name	[en]	*SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*
Name	[es]	*SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

TSP Trade Name

Name	[en]	*SIA*
Name	[es]	*SIA*
Name	[en]	*VATES-A82733262*
Name	[en]	*SISTEMAS INFORMATICOS ABIERTOS S.A.*
Name	[es]	*SISTEMAS INFORMATICOS ABIERTOS S.A.*

PostalAddress

Street Address	[en]	*Avenida de Europa, 2 , Alcor Plaza Edificio B, Parque Oeste Alcorcón*
Locality	[en]	*Alcorcón*
State Or Province	[en]	*Madrid*
Postal Code	[en]	*28922*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*Avenida de Europa, 2 , Alcor Plaza Edificio B, Parque Oeste Alcorcón*
Locality	[es]	*Alcorcón*
State Or Province	[es]	*Madrid*
Postal Code	[es]	*28922*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:info@sia.es*
URI	[en]	*https://psc.sia.es*

TSP Information URI

URI	*[es]*	*https://psc.sia.es/*
URI	*[en]*	*https://psc.sia.es/*

24.1 - Service (granted): Qualified Certificates issued by CA SIA SUB01

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA SIA SUB01*
Name	*[es]*	*Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1422524892*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHIjCCBX6gAwIBAgIEVMoB3DANBgkqhkiG9w0BAQsFADBuMQswCQYDVOQGEwJFUzE4MDYGA1UE
ChMvU0lTVEVNQVMgSU5GT1JNQVRJQ09TIEFCSUVSVE9TIFNPQ0lFREFEIEFOT05JTUExEjAQBgNV
BAUTCUE4MjczMzI2MjERMA8GA1UEAxMIU0lBIFJPT1QwHhcNMTUwMTI5MDk1NjQzWhcNMzAwMTI5
MTAyNjQzWjCBhjELMAkGA1UEBhMCRVMxODA2BgNVBAoTL1NJU1RFTUFTIEIORk9STUFUSUNPUyBB
QkIFUlRPLyBTT0NJRUlRBRCBBTk9OSU1BMRUwEwYDVQQLEwxKVUFMSUZlRUQgQ0ExEjAQBgNVBAUT
CUE4MjczMzI2MjESMBAGA1UEAxMIU0lBIFNVQjAxMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEAIrfsQapsat6SCtT/BMBzpXX/b/1dr7x4Mjt2n4KB94WzL2lcYZ+/KqHBgxOM0s+KThYx
4FIVoCnmt6QWNN/zTN8u5JyVQLsL29w8ISw9e1YZ1nESvBaDNEiZX7W8l4n/OznlSlLGXXSrQvyi
/NcibU9xYlng4NBBSzJbV7uxng8n/C7XmQs/4IsvAgxB+WXL0bGG4zIuRA7oY4ve1t5hTAgRyO4
0zj+UqBWEZgGlsq4vccc9YMU+ErOIRGG87M/ucsOCOG4H5mnWgU/mHaCfOOMnG8woHyc3DdLvBW5
/l0SbkdZIf1/3NGVZAc85uwfZzT47PgrPo9WGW/Y1aAV2zHRWJ3D0bGsxGD/XGq2PrEcHtmoDHtd
GEbDk2Ix/YuoZDnfqQzoxIEjHaB3k10l63Kv5goX/jVXLMMh8nkZys4TayNLpn5RPsZD+yVwTKS
sHVwryxhVGQ5irD1j/wC7nLJcWIqN6XxtFMgNurF56VRIiD3zhL/2rVpO1Bvi/rxdqURDIIkqKfWy
2J+RcAb/+jOojSIhXiSi5+LRGzgG4Ycd4Fj6f33Xbv+0Rh/IsIPf0zgZ43gnPUMSevwwvA2JI/BikNqZ
YqheAavC5YbK+Uz8gKY1FjizDDqtppjYn33eoJWQPt4q6WxsN1kPeelO+gilO+ULBlbEcta+aTdU
fOzGn5sCAwEAAaOCAiEwggIdMA4GA1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMF8G
CCsGAQUFBwEBBFMwUTAqBggrBgEFBQcwAoYcaHR0cHM6Ly9wc2Muc2lhLmVzL2FjX3JhaXouY3J0
MCMGCCsGAQUFBzABhhdoIHRwczovL3BzYy5zaWEuZXMvb2Nzc0C8mwYDVR0gBIGTMIGQMIGNBgRV
HSAAMIGEMB4GCCsGAQUFBwIBFhJodHRwczovL3BzYy5zaWEuZXMwYgYIKwYBBQUHAgIwVhpUQ2Vy
dGlmaWNhZG8gZGUgQUMgc3Vib3JkaW5hZGEuIENvbnN1bHRlIGxhcyBjb25kaWNpb25lcyBkZSB1
c28gZW4gaHR0cHM6L.y9wc2Muc2lhLmVzMIG3BgNVHR8Ega8wgawwK1AcoByGGmh0dHBzOi8vcHNj
LnNpYS5lcy9hcmwuY3JsMIGHoIGEoIGBpH8wTTELMAkGA1UEBhMCRVMxODA2BgNVBAoTL1NJU1RF
TUFTIEIORk9STUFUSUNPUyBBQkIFUlRPLyBTT0NJRUlRBRCBBTk9OSU1BMRUwEAYDVQQFEwlBODI3
MzMyNjIxETAPBgNVBAMTCFNJQSBST09UMQ0wCwYDVQQDEwRDUkwxMB8GA1UdIwQYMBaAFC7gjcIU
rqIbc8nmo0ermWPC7tTwMB0GA1UdDgQWBBTaYNEnMNImhc1+SOL26XkfWjBVrDANBgkqhkiG9w0B
AQsFAAOCAgEAcmCbTQZYHI1AujOmrowGs2fXG0MXWXFZe7AIF7OYVG7G2mr1kbqO+J7HGKUEMnsx
tzIeyitY0+nhePGRooLUyECTFf06RfcyXv/Pk7N4IFQEevGeYg3WHQJWYkKT7mts2HJHFSiL8n/o
sDmwe3V8a2WdmynibVd3NcU9kU5nLtRWPc41wQwo4LYyaIzbZDJXtyu3OnmHwvDtHUucinb6I89b
Zbxn/me0U/hrzl9WNf3dB71nJVJ+Ii94z2EvK2iuyViBYGebwrtB/dFW/Ou1OEgjL mz+qu4rIrXrO
qoTU/IJiSxZTmzlCwBjZhqkOL4M0ojVRBhKNRcYZN6X9OL+0W8SFXC7Yo/q4G2YVgAWejD3W+lm6
ErSAOkyKpKfi/Ar3G31TuTlbWiI1DprdA/qw+pdkX1rw/D0IX0pxa1QQo+ydjKKwLybZKnzCk+
qSDp5GAWbSQwM7rfC+qAs/a5ayg9mazSgbnkY0lmoDE4oIv4S Y+0iXF9oD72H1OVM07/xwJOJw6N
ntGH1AGd5WAyOnREvFVTfPy/y6OJy1qGcHZn6k6TOFBNHVuqWhjVnNHGl+3H19UQkgvv04jwo8/o
TgWMN+iyZT1k5yXp0VZypXE/vPH72A4pODSAmbzQQYM/efbtMK+oSTu6/aXge6QD37QgxlSdnzLj
jVrz7kj/CT8=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *SIA ROOT*

Issuer SERIAL NUMBER: *A82733262*

Issuer O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Issuer C: *ES*

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

Valid from: *Thu Jan 29 10:56:43 CET 2015*

Valid to: *Tue Jan 29 11:26:43 CET 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:96:B7:EC:41:AA:6C:6A:DE:92:0A:D4:FF:04:C0:73:A5:75:FF:6F:FD:5D:AF:BC:78:32:3B:76:9F:82:81:F7:85:B3:2F:62:1C:61:9F:BF:2A:A1:C1:83:13:8C:D2:CF:8A:4E:16:31:E0:59:55:A0:29:E6:B7:A4:16:34:DF:F3:4C:DF:2E:E4:9C:95:40:BB:0B:DB:DC:3C:21:2C:3D:7B:56:19:D6:71:12:BC:16:83:34:48:99:5F:B5:BC:97:89:FF:3B:39:E5:4A:52:C6:5D:74:AB:42:FC:A2:FC:D7:A2:6D:4F:71:60:89:E0:E0:D0:41:4B:3D:E1:57:BB:B1:9E:0F:27:FC:2E:D7:99:0B:3F:E0:8B:2F:02:0C:41:F9:65:CB:D1:B1:86:E3:32:22:B9:10:3B:A1:8E:2F:7B:5B:79:85:30:20:47:23:B8:D3:38:FE:52:A0:56:11:98:06:96:CA:B8:BD:C7:1C:F5:83:14:F8:4A:CE:7D:11:86:F3:B3:3F:B9:EB:0E:08:E1:B8:1F:99:E7:5A:05:3F:9C:76:82:7C:E3:8C:9C:6F:30:A0:7C:9C:DC:3E:0B:BC:15:B9:FE:5D:12:6E:47:59:21:F2:3F:DC:D1:95:64:07:3C:E6:EC:1F:67:34:F8:EC:F8:2B:3E:8F:56:19:6F:D8:D5:A0:15:DB:31:D1:58:9D:C3:D1:B1:AC:C4:60:FF:5C:6A:B6:3E:B1:1C:1E:D9:A8:0C:7B:5D:18:46:C3:93:62:31:FD:8B:A8:64:39:DF:AA:34:33:A3:19:44:8C:76:81:DE:4D:74:23:AD:CA:BF:98:28:5F:F8:D5:5C:B3:0C:87:C9:E4:67:2B:38:4D:AC:8D:2E:99:F9:44:FB:19:0F:EC:95:C1:32:92:B0:75:70:AF:2C:61:54:64:37:8A:B0:F5:8F:FC:02:EE:72:C8:71:62:2A:37:A5:F1:B4:53:20:36:EA:C5:E7:A5:51:22:20:F7:CE:12:FF:DA:B5:69:3B:50:6F:8B:FA:F1:76:A5:11:0C:89:2A:29:F5:B2:D8:9F:91:70:06:FF:FA:33:AC:8D:22:61:5E:24:A2:E7:E2:D1:1A:01:B8:61:E7:78:16:3E:85:DD:76:EF:FB:44:61:26:5C:65:3C:5D:33:81:9E:37:82:73:D4:31:27:AF:C3:00:36:25:40:62:90:DA:99:62:A8:5E:01:AB:C2:E5:86:CA:F9:4C:FC:80:A6:35:16:3B:B3:0C:3A:AD:A6:98:D8:9F:7D:DE:A0:95:90:3E:DE:2A:E9:6C:6C:37:59:0F:79:E9:4E:FA:08:A5:3B:E5:0B:04:86:C4:72:D6:BE:69:37:54:7C:EC:C6:9F:9B:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Info Access

https://psc.sia.es/ac_raiz.crt

https://psc.sia.es/ocsp

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://psc.sia.es

CPS text: [Certificado de AC subordinada. Consulte las condiciones de uso en https://psc.sia.es]

CRL Distribution Points

https://psc.sia.es/arl.crl

C=ES,O=SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA,SERIALNUMBER=A82733262,CN=SIA ROOT,CN=CRL1

Authority Key Identifier *2E:E0:8D:C9:54:AE:A2:1B:73:C9:A6:A3:47:AB:99:63:C2:EE:D4:F0*

Subject Key Identifier *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *68:69:00:54:B9:17:C0:E4:A9:60:92:C4:B3:59:F7:41:80:98:B6:4E:F1:49:A7:0B:78:5A:38:9C:45:51:5D:10*

X509SubjectName

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2020-01-16T01:00:00Z*

24.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

24.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.15*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.16*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.17*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.18*

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.20

Description

24.1.4 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by CA SIA SUB01

Name [es] Certificados Reconocidos emitidos por CA SIA SUB01

Service digital identities

X509SubjectName

Subject CN: SIA SUB01

Subject SERIAL NUMBER: A82733262

Subject OU: QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C: ES

X509SKI

X509 SK I 2mDRJzDSJoXNfkji9ul5H1owVaw=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2019-10-28T01:00:00Z

24.1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

24.1.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

24.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.15*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.16*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.17*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.18*

Description

24.1.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by CA SIA SUB01*
Name	*[es]*	*Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities

X509SubjectName

Subject CN:	*SIA SUB01*
Subject SERIAL NUMBER:	*A82733262*
Subject OU:	*QUALIFIED CA*
Subject O:	*SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*
Subject C:	*ES*

X509SKI

X509 SK I	*2mDRJzDSJoXNfkji9ul5H1owVaw=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2019-08-02T00:00:00Z*

24.1.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

24.1.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.15*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.16*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.17*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.39131.10.1.18*

Description

24.1.6 - History instance n.3 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA SIA SUB01*

Name *[es]* *Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities

X509SubjectName

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *2mDRJzDSJoXNfkji9ul5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-02-15T01:00:00Z*

24.1.6.7 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.6.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

24.1.6.9 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.7

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.15

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.16

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.17

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.18

Description

24.1.7 - History instance n.4 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA SIA SUB01*

Name [es] *Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities

X509SubjectName

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *2mDRJzDSJoXNfkji9ul5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

24.1.7.10 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.8 - History instance n.5 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA SIA SUB01*

Name *[es]* *Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities

X509SubjectName

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *2mDRJzDSJoXNfkji9ul5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-07-06T00:00:00Z*

24.2 - Service (granted): Qualified timestamps issued by TSAQC

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by TSAQC*

Name *[es]* *Sellos de tiempo cualificados emitidos por TSAQC*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1481140816*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHADCCBOigAwIBAgIEWEhqUDANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCRVMxODA2BgNV
BAoT1L1NJU1RFTUFTIEIORk9STUFUSUÑPUyBBQklFUlRPUyBTT0NJRURBRCBBTk9OSU1BMRUwEwYD
VQQLEwxRVUFMSUZJRUQgQ0ExEjAQBgNVBAUTCUE4MjczMzI2MjESMBAGA1UEAxMJU0lBIFNVQjAx
MB4XDTE5MTIwMTExNDI0OVoXDTIwMTIwMTEyMTI0OVowgYgxCzAJBgNVBAYTAkVTMTgwNgYDVQQK
Ey9TSVNURUlBUyBJTkZPUk1BVSIDT1MgQUJJRVJUT1MgU0lDSUVEQUQgQU5PTkINQTEVMBMGA1UE
CxMMUVVBTElGSUVEIENBMRgwFgYDVQRhEw9WQVRFUy1BODI3MzMyNjIxDjAMBgNVBAMTBVRTQVFD
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1mSNqbSphXB3b4AW34ShXSCZJEb3ns1p
yqs1BpNVbUjsLE/CcoCfNrDnV9xO98SCXIl1x3aRRlMHcnSFTOqNhq3oEvwH95+J9QNKKv+a8kv4
ctkXjczZtt/zfreKH95WQ1n2EVlMbgm0tuk6UygcdFePL4tbW0MuQ4HpQ7YTagnzXkIUdTV5vLyN
zVY0RCAAMCesN9eQIVKGwgATUhnNAfQIbOZduZHvo/6IdLuuSJAKIdSRdb6V9+v0EwoX/bVvVQp
nRJai21sjL2KUbydO/wa6WgtdZ+Q6gygNFAW6M5pxxmQF3ZYT/EhHf9l/Jh0i2dZ26BUhh1qV7Yr
UyENlQIDAQABo4ICcDCCAzmwwDgYDVR0PAQH/BAQDAgbAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMI
MFAGA1UdHwRJMEcwRaBDoEGGH2h0dHBzOi8vcHNjLnNpYS5lcy9hY19zdWIwMSSjcmyGHmh0dHA6
Ly9wc2Mufac2lhLmVzL2FjX3N1YjAxLmNybDBgBggrBgEFBQcBAQRUMFIwIwYIKwYBBQUHMAWGF2h0
dHBzOi8vcHNjLnNpYS5lcy9vY3NwMCsGCCsGAQUFBzAChh9odHRwczovL3BzYy5zaWEuZXMvYWNf
c3ViMDEuY3J0MIHwBgNVHSAEgegwgeUwgdcGCysGAQQBgrFbCgEOMIHHMB4GCCsGAQUFBwIBFhJo
dHRwczovL3BzYy5zaWEuZXMwgaQGCCsGAQUFBwICMGXDIGÚQ2VydGlmaWNhZG8gZGUgc2Vydmlj
aW8gZGUgZXbwZWRpY2mIb24gZGUgc2VsbG9tZGVsZWNkcsOzbmljb3MgY3VhbGlmaWNhZG9zIGRl
IHRpZW1wby4gQ29uZGljaW9uZXMgZGUgdXNvIHkgdsOtYXMgZGUgY29udGFjdG8gZW46IGh0dHBz
Oi8vcHNjLnNpYS5lczAJBgcEAIvsQAEBMHoGCCsGAQUFBwEDBG4wbDAIBgYEAI5GAQEwCwYGBACO
RgEDAgEPMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwJwYGBACORgEFMB0wGxYVaHR0cHM6Ly9wc2Mu
c2lhLmVzL2VqEwJlbATBgYEAISGAQYwCQYHBACORgEGAjAfBgNVHSMEGDAWgBTaYNEnMNImhc1+
SOL26XkfWjBVrDANBgkqhkiG9w0BAQsFAAOCAgEAe4dW1YL1uTYwcHXFRDulBvFcbLrWcYSBedEo
m9mkIL+FAFkkz3kFox9iudSoDUcri3M6YmwA0lBwIFm3mJ9aN5GH+Sa6+XhXbYKXzqmhdx0oCBjm
GMsKs0m29OzP1m55ftnoKpGa9qBx09RJMcUY1+9dqDh3yMcdIAsy1dlkV3NLt1YdtFb1+ms80Jbsj
vBs92U3b+qZx9T7G80mZNSyal84wgQwCsBhCuzzypAiHoiuZ7Muren7BHwSu+vjnVtP5gtWtF0
81dUg75GlBFgkIg4ru0CF4sFgrRhbLX2H8PEXYyyyTPe8bd1szqwrHKMEGWIV3z/0zvZwa1Kci3
/5UWo/uFWd/f3FJQbpNzCqY/pV7H/EFkbdirK1u6FzAyV7hfhJZ62Cj4sIOlbvZqgwwakM4XMRawT
peGBXdbA4CrwITb4VL2c/3AKPFY/TQ7NGyDal7QcdIDaSA2H3kgUo1rMkRwzlzm93AZJaVQcAt+u
w0zki/M36RtEURjox0KW+c52Zl8skElGocVXz4OcexZxyPawYKFz7IwIB1UboPQcsaMP/gZJJldk
hr+IbnPz3qrUxVYhkgzfBNCNx2ehXMV3GrZSIP5VnWnIlBQBeSHJDpahDM51YNgzp4w+nDJfR4GH
x8Gl5Ht0NmAo+XU/gfNQZR1dzsEJh6ibZeTfwwbA=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *SIA SUB01*

Issuer SERIAL NUMBER: *A82733262*

Issuer OU: *QUALIFIED CA*

Issuer O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Issuer C: *ES*

Subject CN: *TSAQC*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

Valid from: *Fri Dec 01 12:42:49 CET 2017*

Valid to: *Tue Dec 01 13:12:49 CET 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D6:64:8D:A9:B4:A9:85:70:77:6F:80:16:DF:84:A1:5D:20:99:24:46:F7:9E:CD:69:CA:AB:35:06:93:55:6D:48:EC:2C:4F:C2:72:80:9F:36:B0:E7:57:DC:4E:F7:C4:82:5C:82:35:C7:76:91:46:53:07:72:74:85:4C:EA:8D:86:AD:E8:12:FC:07:F7:9F:89:F5:03:4A:2A:FF:9A:F2:4B:F8:72:D9:17:8D:EC:D9:B6:DF:F3:7E:B7:8A:1F:DE:56:43:59:F6:11:59:4C:6E:09:B4:BA:4E:94:CA:07:1D:15:E3:CB:E2:D8:56:D0:CB:90:7F:89:69:43:B6:13:6A:09:F3:5E:42:14:75:35:79:BC:BC:8D:CD:56:34:44:20:22:33:77:AC:37:D7:10:21:52:86:C2:00:13:D2:F9:CD:01:F4:09:6C:E6:5D:B9:91:EF:A3:FE:88:7D:D2:EE:B9:22:40:2B:57:79:45:DD:3A:57:DF:B2:D0:4C:28:5F:F6:D5:AD:54:29:9D:12:5A:8B:6D:6C:8C:BD:8A:51:BC:9D:3B:FC:1A:E9:68:2D:75:9F:90:EA:0C:A0:34:50:16:E8:CE:69:C7:19:90:17:76:58:4F:F1:21:1D:FF:65:FC:98:74:8B:67:59:DB:A0:54:86:1D:6A:57:B6:2B:53:21:0D:95:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points

https://psc.sia.es/ac_sub01.crl

http://psc.sia.es/ac_sub01.crl

Authority Info Access

https://psc.sia.es/ocsp

https://psc.sia.es/ac_sub01.crt

Certificate Policies

Policy OID: 1.3.6.1.4.1.39131.10.1.14

CPS pointer: https://psc.sia.es

CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es]

Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

Authority Key Identifier *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *94:6B:BF:53:5A:21:D9:D7:32:E3:E5:70:B6:2E:79:3B:3A:09:22:21:35:7C:E1:B2:FA:61:C7:16:95:80:2D:38*

Certificate fields details

Version: *3*

Serial Number: *1481668284*

X509 Certificate

-----BEGIN CERTIFICATE-----

*MIIG/DCCBOSgAwIBAgIEWFB2vDANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCRVMxODA2BgNV
BAoTL1NJU1RFTUFTIEIOR&9STUFUSUNPUyBBQklFUlRPUyBTT0NJRURBCBBT1k9OSU1BMRUwEwYD
VQQLEwxRVUFMSUZRUQgQ0ExEjAQBgNVBAUTCUE4MfczMzI2MjESMBAGA1UEAxMUU0IBIFNVQjAx
MB4XDT1wMDkwNDExNTQwMVoXDTIzMDkwNDEyMjQwMVowg1gxCzAJBgNVBAYTAkVTMTgwNgYDVQQK
Ey9TSVNURU1BUyBJTkZPUk1BVEIDT1MgQUJJRVJUT1MgU09DSUVEQUQgQU5PTkINQTEVMBMGA1UE
CxMMUVVBTElGSUVEIENBMRgwFgYDVQRhEw9WQVRFUy1BODI3MzMyNjIxDjAMBgNVBAMTBVRTQVFD
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1mSNqbSphXb3b4AW34SbXSCZJEb3ns1p
xqs1BpNVbU/jsLE/CcoCINzDnV9xO98SCXII1x3aRRIMHzcSFTOqNhq3oEvwH95+J9QNKKv+a8kv4
ctkXjczZtt/zfrcKH95WQ1n2EVIMbgm0uk6UygcdFcPL4thW0MuQf4lpQ7YTagnzXkUdTV5vLyN
zVY0RCAiM3csN9cQIVKGwgATfvnNAtQJb0ZduZHvo/6IfdLuuSJAK1d5Rd06V9+y0EwoX/bVrVQp
nRJai21sjL2KUbydO/wa6WgtdZ+Q6gygNFAW6M5pxxmQF3ZYT/EhH19l/Ih0i2dZ26bUhh1qV7Yr
UyENIQIDAQABo4IC5DCCAmgwDgYDVR0PAQH/BAQDAgbAMB8YGA1UdIQEB/wQMMAoGCCsGAQUFBwMI
MGAGCCsGAQUFBwEBBFQwUjAjBggrBgEFBQcwAYYXaHR0cHM6Ly9wc2Muc2lhLmVzL29jc3AwKwYI
KwYBBQUHMAKGH2h0dHBzOi8vcHNjLnNpYS5lcy9hY19zdWIwMS5jcnQwgfAGA1UdASB6DCB5TCB
1wYLKwYBBAGCsVsKAQ4wgccwHgYIKwYBBQUHAgEWEmb0dHBzOi8vcHNjLnNpYS5lczCBpAYIKwYB
BQUIAgIwgZcMgZRDZXJ0aWZpY2FkbyBkZSBzZXJ2aWNpbyBkZSBlcHBlZGljaCBhIBkZSBzZWxs
b3MgZWxlY3Ryw7NuaWNvcyBjdWFsaWZpY2Fkb3MgZGUgdGllbXBvLiBDb25kaWNpb25lcyBkZSB1
c28geSB2w61hcyBkZSBjb250YWN0byBlbjogaHR0cHM6Ly9wc2Muc2lhLmVzMAkGBwQAi+xAAQEw
egYIKwYBBQUHAQMEbjBsMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wFQYIKwYBBQUHCwIwCQYHBACL
7EkBAjAnBgYEAI5GAQUwHTAbFhVodHRwcwL3BzYy5zaWEuZXMvZW4TAmVuMBMGBgQAjkYBBjAJ
BgcEAI5GAQYCMEwGA1UdHwRFMEMwQaA/oD2GHGh0dHA6Ly9wc2Muc2lhLmVzL2NybGMxMC5jcmyG
HWh0dHBzOi8vcHNjLnNpYS5lcy9jcmxjMTAuY3JsMB8GA1UdIwQYMBaAFNpg0Scw0iaFzX5I4vbp
eR9aMFWsMA0GCSqGSIb3DQEBCwUAA4ICAQBS1Z0eTMfzj/PesFOyHmecsMJZ/IDAQh+eV73zp76U
QcTHbFkYXhb2YceQ4MYykkJpdXVqm9TR/OIIsmElpYLa1iw3YRmwSeg9y4RsHyqiRhIi+mXYWsmY
lpYYw1C23hL+KgxC9HfhXEt7QFugdIYv+SbLErC1tyXrQ3n1335TrSGUOkcpGoYwmmAQf7SxudAY
nH3h5Fi9R5p1wxjZQwigDy5HzsxwncOvqPD6sJUpyrQb+t9ZFbaF7Yob5P+lOh2aEME8/lMG0M1j
9Z4WYSWFY5CghgbereUwlvFddYeE4ktIo8DvgLTTNrSYRq20NvpiKFbDIEpMCaptD8fLQiWaDPp
U667SYpV7KFa6MIlW7TdoCb15mlh8zG5n6+GgNG7+cZaeVHYXbo8eUu8fZR0U/h5vSyLqjkBwu/A
vPjKILXCMCit2wpYA3dc2KU0MFhZYHVpRo+qofHLmqkenDu2TbPZoB/NCUa4r1WTsoXRTlDo3sRQ
LXi9EPzLRp75VBVyCIRETq4AlzKKG6kjQnbb0zEe+oqI2y5++RYtPtXlHOo2qq1wGptvIqlMT8zD
n+Z7tz63RsoUwC71KUSpzu75pebPLWga2M/4c8XAAos/qq5b6BMwenMnPIxIAI8Q0e+tsk9WOQRQ
a2yyg6I/bzNPJHODWl5B95OTtrlnFtuMw==*

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*SIA SUB01*
Issuer SERIAL NUMBER:	*A82733262*
Issuer OU:	*QUALIFIED CA*
Issuer O:	*SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*
Issuer C:	*ES*
Subject CN:	*TSAQC*
Subject 2.5.4.97:	*VATES-A82733262*
Subject OU:	*QUALIFIED CA*
Subject O:	*SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*
Subject C:	*ES*
Valid from:	*Fri Sep 04 13:54:01 CEST 2020*
Valid to:	*Mon Sep 04 14:24:01 CEST 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D6:64:8D:A9:B4:A9:85:70:77:6F:80:16:DF:84:A1:5D:20:99:24:46:F7:9E:CD:69:CA:AB:35:06:93:55:6D:48:EC:2C:4F:C2:72:80:9F:36:B0:E7:57:DC:4E:F7:C4:82:5C:82:35:C7:76:91:46:53:07:72:74:85:4C:EA:8D:86:AD:E8:12:FC:07:F7:9F:89:F5:03:4A:2A:FF:9A:F2:4B:F8:72:D9:17:8D:EC:D9:B6:DF:F3:7E:B7:8A:1F:DE:56:43:59:F6:11:59:4C:6E:09:B4:BA:4E:94:CA:07:1D:15:E3:CB:E2:D8:56:D0:CB:90:7F:89:69:43:B6:13:6A:09:F3:5E:42:14:75:35:79:BC:BC:8D:CD:56:34:44:20:22:33:77:AC:37:D7:10:21:52:86:C2:00:13:D2:F9:CD:01:F4:09:6C:E6:5D:B9:91:EF:A3:FE:88:7D:D2:EE:B9:22:40:2B:57:79:45:DD:3A:57:DF:B2:D0:4C:28:5F:F6:D5:AD:54:29:9D:12:5A:8B:6D:6C:8C:BD:8A:51:BC:9D:3B:FC:1A:E9:68:2D:75:9F:90:EA:0C:A0:34:50:16:E8:CE:69:C7:19:90:17:76:58:4F:F1:21:1D:FF:65:FC:98:74:8B:67:59:DB:A0:54:86:1D:6A:57:B6:2B:53:21:0D:95:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Authority Info Access	*https://psc.sia.es/ocsp* *https://psc.sia.es/ac_sub01.crt*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.39131.10.1.14* *CPS pointer: https://psc.sia.es* *CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es]* *Policy OID: 0.4.0.194112.1.1*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
CRL Distribution Points	*http://psc.sia.es/crlc10.crl* *https://psc.sia.es/crlc10.crl*
Authority Key Identifier	*DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*
Key Usage:	*digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *55:A4:10:9A:4E:AA:63:B6:46:1F:DB:B1:1E:1C:0B:AD:A6:E1:8C:DA:DB:45:4F:E5:63:A7:D3:6F:18:BF:57:1C*

X509SubjectName

Subject CN: *TSAQC*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *nrZ7bmnQvpA1gs5HCLWNwxsusSE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-02-15T01:00:00Z

24.3 - Service (granted): Servicio cualificado de entrega electrónica certificada "SIAVAL"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description

[en] *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name *[es]* *Servicio cualificado de entrega electrónica certificada "SIAVAL"*

Name *[en]* *Qualified electronic registered delivery service "SIAVAL"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1481574354*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHpDCCBYygAwIBAgIEWE8H0jANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCRVMxODA2BgNV
BAoMLlNJUlRFTUFTIEtlORk9STUFUSUNPUyBBQklFUlRPUyBTT0NJRUlRBRCBBTk9OSUlBMRUwEwYD
VQQLDAxRVUFMSUZlRUQgQ0ExEjAQBgNVBAUTCUE4MjczMzI2MjESMBAGA1UEAwwJU0lBIFNVQjAx
MB4XDTE5MTEyMDA5MzExMloXDTIyMTEyMDEwMDExMlowgYIxCzAJBgNVBAYTAkVTMSwwKgYDVQQK
DCNTSVNURU1BUyBJTkZPUk1BVElDT1MgQUJlRVJUT1MgUy5BLjEYMBYGA1UEYQwPVkFURVMtQTgy
NzMzMjYyMRowGAYDVQQLDBFTRUxMTyBFTEVDVFJPTklDTzEPMA0GA1UEAwwGU0lBVkFMMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApu0rWuquBtVKTSOrv3P5kf4lurV33vypSawWC2vD
UffzPcE+jm00/FquvC4e3bfqqDovU5ni4wjkUQzRpguBhHEaz7Rzmbe8RczMns6Bk3LmG7xOYm3U
V7QIl7hmzm1Z7k2v/szlj4ssewurBrveHznfW26cWeh3g6Hoke5uwWj7uxkz2UqvJ9S/Ju5T0kNJ
3ISKB4VtXaLqluK7dmOUpUs3ChC4YP0VT+yKXOwCTtkvqSRLF2Rk4Gtt30Hqt7BJrcOB45a8VpA/
ODZ/ddzDHbPuCb7uscYA2REA6QNuJfMVA6u8DwDU1Y4ZZBxnEtOum2r/9E++y4cTSg+LvSpt0SwID
AQABo4IDGjCCAxYwgZYGA1UdEQSBjzCBi6SBiDCBhTExMC8GCysGAQQBgrFbCgIGDCNTSVNURU1BUyBJTkZP
TEVDVFJPTkIDTyBERSBOSVZFTCBNRURJTzE0MDIGCysGAQQBgrFbCgIGDCNTSVNURU1BUyBJTkZP
Uk1BVEIDT1MgQUlJRVlUT1MgUy5BLjEaMBgGCysGAQQBgrFbCgIHDAIBODI3MzMyNjIwDgYDVR0P
AQH/BAQDAgPoMB0GA1UdJQWMBiQGCCsGAQUFBwMCBggrBgEFBQcDBDBgrBgrBgEFBQcBAQRUMFIw
IwYIKwYBBQUHMAGGF2h0dHBzOi8vcHNjLnNpYS5lcy9vY3NwMCsGCCsGAQUFBzAChh9odHRwczov
L3BzYy5zaWEuZXMvYWNfc3ViMDEuY3J0MIHhBgNVHSAEgdkwgdYwgbwGCysGAQQBgrFbCgEMMIGs
MB4GCCsGAQUFBwIBFhJodHRwczovL3BzYy5zaWEuZXMwgYkGCCsGAQUFBwICMH0Me0NlcnRpZmlj
YWRlcGNlYWxpZmlj YWRvIGRlIFNlbGxvIEVsZWNlcsOzbmljbyBkZSBuaXZlbCBtZWRpby4gQ29u
ZGljaW9uZXMgZGUgdXNvIHkgdsOtYXMgZGUgY29udGFjdGi8gZW46lGh0dHBzOi8vcHNjLnNpYS5l
czAJBgcEAIvsQAEBMAoGCGCFVAEDBQYCMHoGCCsGAQUFBwEDBG4wbDAIBgYEAI5GAQEwCwYGBACO
RgEDAgEPMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwJwYGBACORgEFMB0wGxYVaHR0cHM6Ly9wc2Mu
c2lhLmYzL2VuEuJlbjATBgYEAI5GAQYwCQYHBACORgEGAjBKBgNVHR8EQzBBMD+gPaA7hhtodHRw
Oi8vcHNjLnNpYS5lcy9zcmxjNCSjcmyGHGh0dHBzOi8vcHNjLnNpYS5lcy9zcmxjNCSjcmwwHwYD
VR0jBBgwFoAU2mDRJzDSJoXNfkji9uI5H1owVawwHQYDVR0OBBYEFMOTo2cQFvwgeYuL5T/6gewT
6CCKMA0GCSqGSIb3DQEBCwUAA4ICAQAUYHMoTbxWYRVeEmO/ptqxFhifxU2VecWKnKoISl91erlR
PLdotI9bHHkldqWyZApzqDWVUneLYB9/mjq5XEsrbqIZtjBTMgwykbF3BktC5rJzAC/uCVoEIVuO
EDQLDjsKOXpSHCU/ok/tkIw2ucBZf6qWTAoz7z0AU1/yeRZaNoFnIAb7HRlhpnGgH3Qsi7Wukso
cU40BVnEgBl7m//tZVsvqLEB3ev9nN0oz4drB5ivhisn6NBBPeqFNhPDHZSzS6zlsca/B0cVrMTw
wXqDfXUcZJI4Pn1hC8oL6Zy0dPbhOHXg8MfvMyTbxOKcLwU/nklsucLKvT4SbD9dWbvKiSRA/mEfi
ARwdJkw4M17Qxqm0gFK52wv8SL+BqMQCelZMwm7OZvHJ2sXFn/nhgCMfAc22ccLmD5xOT1XzMkf
Fn8bN4yGzjkNXZnKDcwYoGTyoCn/MYL9cMRgwrQUoCa1Bj1+G0VrbHjQEVZjxEzNL1sfNEFsoB
jWD7cl7iM4P4FYoASJYG8rF5laodz5zTXPx0pvHfZlg5TMQEmQftu4pUB1muWujf4EQwDVtGQ0w
y405xVKrSlc+kv02msE76dqFgcL/cKkToikN6Rzd1V7Fm/E+1D/bh2qcQPXF5Hbr3n7x2SgFm+BC
hBgZC9fHxk7wfuNPIAqYOmN7sNBlvQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *SIA SUB01*

Issuer SERIAL NUMBER: *A82733262*

Issuer OU: *QUALIFIED CA*

Issuer O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Issuer C: *ES*

Subject CN: *SIAVAL*

Subject OU: *SELLO ELECTRONICO*

Subject 2.5.4.97: *VATES-A82733262*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS S.A.*

Subject C: *ES*

Valid from: *Wed Nov 20 10:31:12 CET 2019*

Valid to: *Sun Nov 20 11:01:12 CET 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A6:ED:2B:5A:EA:AE:05:F5:4A:4D:23:AB:BF:73:F7:91:FE:25:C2:B5:77:DE:FC:A9:49:AC:16:0B:6B:C3:51:F7:F3:3
D:C1:3E:8E:6D:34:FC:5A:AE:BC:2E:1E:DD:B7:EA:A8:3A:2F:53:99:E2:E3:08:E4:51:0C:D1:A6:0B:81:84:71:1A:CF:B4:73:99:B7:BC:45:CC:CC:9E:CE:81:93:72:E6:1B:BC:4E:62:6D:D4:57:B4:08:23:B8:66:CE:6D:59:EE:4
D:AF:FE:CC:E5:8F:8B:2C:7B:0B:AB:06:BB:DE:1F:39:DF:5B:6E:9C:59:E8:77:83:A1:E8:91:EE:6E:C1:68:FB:BB:19:33:D9:4A:AF:27:D4:BF:26:EE:53:D2:43:49:DC:84:8A:07:85:6D:5D:A2:EA:96:E2:BB:76:63:94:A5:4B:3
7:0A:10:B8:60:FD:15:4F:EC:8A:5C:EC:02:4D:F9:2F:A9:24:B:17:64:64:E0:6B:5F:DF:41:EA:7F:B0:49:AD:C3:81:E3:96:BC:56:90:3F:38:36:7F:75:D8:03:1D:B3:DA:09:BE:EE:B1:C5:40:D9:11:00:E9:03:6E:25:F3:15:03:AB
:BC:0F:00:D4:D5:8E:36:64:1C:67:12:33:9A:9B:6A:FF:F4:4F:B2:E1:C2:13:4A:0F:8B:BD:2A:74:4B:02:03:01:00:01

Subject Alternative Name *OID.1.3.6.1.4.1.39131.10.2.7=A82733262, OID.1.3.6.1.4.1.39131.10.2.6=SISTEMAS INFORMATICOS ABIERTOS S.A., OID.1.3.6.1.4.1.39131.10.2.1=SELLO ELECTRONICO DE NIVEL MEDIO*

Extended Key Usage *id_kp_clientAuth*

Authority Info Access *https://psc.sia.es/ocsp*

https://psc.sia.es/ac_sub01.crt

Certificate Policies	*Policy OID: 1.3.6.1.4.1.39131.10.1.12* *CPS pointer: https://psc.sia.es* *CPS text: [Certificado cualificado de Sello Electrónico de nivel medio. Condiciones de uso y vías de contacto en: https://psc.sia.es]* *Policy OID: 0.4.0.194112.1.1* *Policy OID: 2.16.724.1.3.5.6.2*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
CRL Distribution Points	*http://psc.sia.es/crlc4.crl* *https://psc.sia.es/crlc4.crl*
Authority Key Identifier	*DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*
Subject Key Identifier	*C3:93:A3:67:10:16:FC:2A:81:8B:8B:E5:3F:FA:81:EC:13:E8:20:8A*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment - keyAgreement*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B5:AA:55:A4:C5:50:58:F0:AE:92:63:96:18:EE:D9:F1:5D:63:F8:54:63:78:03:8A:9D:BD:92:9A:CB:4E:1B:52*

X509SubjectName

Subject CN:	*SIAVAL*
Subject OU:	*SELLO ELECTRONICO*
Subject 2.5.4.97:	*VATES-A82733262*
Subject O:	*SISTEMAS INFORMATICOS ABIERTOS S.A.*
Subject C:	*ES*

X509SKI

X509 SK I	*w5OjZxAW/CqBi4vlP/qB7BPoIIo=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-12-10T01:00:00Z

25 - TSP: COLORIURIS, S.L

.

TSP Name

Name	[en]	*COLORIURIS, S.L*
Name	[es]	*COLORIURIS, S.L*

TSP Trade Name

Name	[en]	*Coloriuris, Prestador de Servicios de Confianza (CIPSC)*
Name	[es]	*Coloriuris, Prestador de Servicios de Confianza (CIPSC)*
Name	[en]	*VATES-B99091696*
Name	[en]	*Coloriuris S.L.*

PostalAddress

Street Address	[en]	*C/ Alfonso I nº 23, entresuelo centro*
Locality	[en]	*Zaragoza*
State Or Province	[en]	*Zaragoza*
Postal Code	[en]	*50003*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*C/ Alfonso I nº 23, entresuelo centro*
Locality	[es]	*Zaragoza*
State Or Province	[es]	*Zaragoza*
Postal Code	[es]	*50003*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*https://cipsc.coloriuris.net/*
URI	[en]	*mailto:info@coloriuris.net*
URI	[es]	*mailto:info@coloriuris.net*

URI	*[es]*	*https://cipsc.coloriuris.net/*

TSP Information URI

URI	*[en]*	*https://cipsc.coloriuris.net/*
URI	*[es]*	*https://cipsc.coloriuris.net/*

25.1 - Service (withdrawn): Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física*
Name	*[es]*	*Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *706445458326489759*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIeTCCBmGgAwIBAgIICc3MZsS9Cp8wDQYJKoZIhvcNAQELBQAwgdsxIzAhBgkqhkiG9w0BCQEW
FGNpcHNjQGNvbG9yaXVyaXMubmV0MTgwNgYDVQQDDC9DSVBTQyAtIFJhw616IGRlIGxhIEF1dG9y
aWRhZCBkZSBDZXJ0aWZpY2FjaC0zbjESMBAGA1UEBRMJQjk5MDkxNjk2MSwwKgYDVQQLDCNQcmVz
dGFkb3lgZGUgU2VydmlaW9zIGRlIENvbmZpYW56YTEYMBYGA1UECgwPQ29sb3JpdXJpcyBTLkwu
MREwDwYDVQQHDAhaYXJhZ296YTELMAkGA1UEBhMCRVMwHhcNMTUwNzE0MTAxNTEwHhcNMjUwNzE0
MTAxNTEwWjCB7zEjMCEGCSqGSIb3DQEJARYUY2Iwc2NAY29sb3JpdXJpcy5uZXQxTDBKBgNVBAMM
Q0NJUFNDIC0gU3VyYXV0b3JpZGFkIGNlcnRpZmlj YWRvcyBkZSBwZXIz
b25hIGbDrXNpY2ExEjAQBgNVBAUTCUI5OTA5MTY5NjEsMCoGA1UECwwjUlJlc3RhZG9yIGRlIFNl
cnZpY2lvcyBkZSBDb25maWFuemExGDAWBgNVBAoMD0NvbG9yaXVyaXMgUy5MLjERMA8GA1UEBwwI
WmFyYWdvcmExCzAJBgNVBAYTAkVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4zvQ
d7TyIBUkFHuqxDb2oNzJLrQNjRFsaa6WvXwbUfQyo3XMBR0wDm7Arb2L1FJComkMTnrTGz3wQ1
nJiccqh1sbr5oh+AEIMuzPg7VBr3J6gKDabFq0e1Wbmw1M3Qe16WTID+jbNiBZMDpmlfzIFbvlw
8+TI6iPVczDjZ4w7RB5cCtIH9ShdH6yY62SFMuPjxwIQuNhHUcvRj5+Wr1sIsUE+RxhhullF39rM
+/Stv9bja3tCCMRspzK4YpmUT8OZVPGkCJPA5DlgS6TJ52PJL5MSQOgttLWQJnhaQFFzQEOIlovu
9wMcP4elex2kOJBFkCHJlkM9bEMi95MNVQJDAQABo4IDKTCCAyUwegYIKwYBBQUHAQEEbjBsMEEG
CCsGAQUFBzAChjVodHRwczovL2NpcHNjLmNvbG9yaXVyaXMubmV0L2NlcnRpZmljYWRvcy9hYy9y
YW16LmNydDAnBggrBgEFBQcwAYYbaHR0cHM6Ly9vY3NwLmNvbG9yaXVyaXMubmV0MB0GA1UdDgQW
BBQC6WovsgXTG2P7PMDFkmoLy2DKTAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFHkb4Vyh
8ZZS16A2Wa0pavkNnGmMIIBGwYDVR0gBIIBEjCCAQ4wggEKBg0rBgEEAYKnIwADAQIAMIH4MHHA
BggrBgEFBQcCAjCBxx6BsABTAHUAYgBBAHUAdABvAHIAaQBkAGEAZAAgAEMASQBRQAFMAQwAgAHAA
YQByAGEAIABlAG0AaQBzAGkA8wBuACAAZABlACAAYwBlAHIAdABpAGYAaQBjAGEAZABvAHMAIABk
AGUAIABmAGkAcgBtAGEAIABlAGwAZQBjAHQAcgDzAG4AaQBjAGEAIABwAGEAcgBhACAAcABlAHIA
cwBvAG4AYQAgAGYA7QBzAGkAYwBhMDMGCCsGAQUFBwIBFidodHRwczovL2NpcHNjLmNvbG9yaXVy
aXMubmV0L3BvbGl0aWNhcy8wggEIBgNVHR8EggEcMIIBGDCCARSgLqAshjpodHRwczovL2NpcHNj
LmNvbG9yaXVyaXMubmV0L2NybC9hYy9hYy5jcmyigeGkgd4wgdsxIzAhBgkqhkiG9w0BCQEWFGNp
cHNjQGNvbG9yaXVyaXMubmV0MTgwNgYDVQQDDC9DSVBTQyAtIFJhw616IGRlIGxhIEF1dG9yaWRh
ZCBkZSBDZXJ0aWZpY2FjaC0zbjESMBAGA1UEBRMJQjk5MDkxNjk2MSwwKgYDVQQLDCNQcmVzdGFk
b3lgZGUgU2VydmlaW9zIGRlIENvbmZpYW56YTEYMBYGA1UEGwPQ29sb3JpdXJpcyBTLkwuMREw
DwYDVQQHDAhaYXJhZ296YTELMAkGA1UEBhMCRVMwDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3DQEB
CwUAA4ICAQAAEsu6K2Cen4eJvFMZ+b/i8qCdi18lqKoAnDORCmSt5AYTIjsOGWZJIgYhZOjFONYt
hmrqjIJ2ZQEOCJWl3pBgMJbCuDtGpJNNjQ8ku+F1Lr/EH623WrWZ9D16qGW8MMXFDqrCOUfrPOsR
izun+HBd+pJcqAizLvNZdUZMZdQUAG1Rp+ua9t0/+5dG9MVAosSgXTINaZXs8Ya+qX8m/AiOeyB2
IQQ0GtBdkPtdlIDIS+7q9KB9oHhnp3+073oSz2WihtaauEm1TuzwRBDIGzJ7AzYdroF9VamQwGxz
fCBK1uu6lBstVbKAGS50zQSpEQjzbtAKlIWNhp0JlyPJd9s9GAVZoYuW1L/buTTmqDmQvsKAO5sK7
hk23GCKDw3fJqDp08rG00LHwPhWdVEBL+kUMLKEIoYXo4RwNdPGOUSQfPhJHSakSsQ9nbdZUa5Tn
zukcCVVr5FdpJb8WLVpPQAkmPlvbgEDKovyRzQpmqBXBFbE8upYs9Kp78ETaa0R81u/BFKuo0QE
DjaNpDwLU8GHOTB/dIOKLVGJHo+rfykKtSMBr6rgm7D77rUM9bbH4mJhvt7I5qISSp2n2G3HAOQJGv
BZEB04JbEK8cwOcZSTdhielYprkWA33PCXjGQst2jDRwC5VJ7XkxArP9QQsZXVOXFxp2Z7Yrxvoe
jZLkk5GDFg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L:	*Zaragoza*
Issuer O:	*Coloriuris S.L.*
Issuer OU:	*Prestador de Servicios de Confianza*
Issuer SERIAL NUMBER:	*B99091696*
Issuer CN:	*CIPSC - Raíz de la Autoridad de Certificación*
Issuer E:	*cipsc@coloriuris.net*
Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject OU:	*Prestador de Servicios de Confianza*
Subject SERIAL NUMBER:	*B99091696*
Subject CN:	*CIPSC - Subautoridad de emisión de certificados de persona física*
Subject E:	*cipsc@coloriuris.net*
Valid from:	*Tue Jul 14 12:15:10 CEST 2015*
Valid to:	*Mon Jul 14 12:15:10 CEST 2025*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E3:3B:D0:77:B9:58:C8:80:54:90:5D:2E:AB:10:DB:DA:83:60:24:BA:D0:36:34:45:B1:A6:BA:5A:2B:D7:C1:B5:1F:43:2A:13:F0:C0:51:D3:00:E6:EC:09:FD:CC:BD:45:24:2A:26:90:C4:E7:AD:31:B3:DF:04:35:9C:98:9C:72:A8:75:B1:BA:F9:A2:1F:80:10:83:2E:CC:F8:13:54:1A:F7:27:A8:0A:0D:A6:C5:AB:47:B5:59:BA:E7:C3:53:37:41:ED:7A:59:39:43:FA:36:CD:88:16:4C:0E:99:A5:7F:32:05:6E:F9:70:F3:E4:C8:EA:23:D5:73:30:E3:67:8C:3B:44:1E:5E:0A:D9:47:F5:28:5D:1F:AC:98:EB:64:85:32:E3:E3:C7:02:10:B8:D8:47:51:CB:D1:8F:9F:96:AF:5B:08:B1:41:3E:47:18:61:BA:52:05:DF:DA:CC:FB:F4:AD:BF:D8:63:6B:7B:42:08:C4:6C:A7:32:B8:62:99:94:4F:C4:19:54:F1:A4:08:93:C0:E4:39:60:4B:A4:C9:E7:63:C9:2F:93:12:40:E8:2D:B4:B5:90:26:78:5A:40:51:73:40:43:A5:96:8B:EE:F7:03:1C:3F:87:A5:7A:FD:A4:38:90:45:90:21:C9:90:CF:65:88:43:22:F7:93:0D:55:02:03:01:00:01*
Authority Info Access	*https://cipsc.coloriuris.net/certificados/ac/raiz.crt* *https://ocsp.coloriuris.net*
Subject Key Identifier	*02:E9:6A:2F:B2:05:D3:1B:63:FB:3C:C0:C5:92:6A:0B:FF:2D:83:29*
Basic Constraints	*IsCA: true*
Authority Key Identifier	*79:21:E1:5C:A1:F1:96:7C:D7:A0:36:89:66:B4:A5:AB:E4:36:71:A6*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.37799.0.3.1.2.0* *CPS text: [SubAutoridad CIPSC para emisión de certificados de firma electrónica para persona física]* *CPS pointer: https://cipsc.coloriuris.net/politicas/*

CRL Distribution Points *https://cipsc.coloriuris.net/crl/ac/ac.crl*

CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz de la Autoridad de Certificación,SERIALNUMBER=B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D8:23:77:C5:2B:28:D8:A9:39:40:35:B2:8B:71:3A:62:1C:C0:49:DA:5E:BC:D1:7F:F9:A3:8C:5F:25:EA:1A:6D*

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject SERIAL NUMBER: *B99091696*

Subject CN: *CIPSC - Subautoridad de emisión de certificados de persona física*

Subject E: *cipsc@coloriuris.net*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-07-01T22:00:00Z

25.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.1.2 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name *[en]* *Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física*

Name	*[es]*	*Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject OU:	*Prestador de Servicios de Confianza*
Subject SERIAL NUMBER:	*B99091696*
Subject CN:	*CIPSC - Subautoridad de emisión de certificados de persona física*
Subject E:	*cipsc@coloriuris.net*

X509SKI

X509 SK I	*AulqL7IF0xtj+zzAxZJqC/8tgyk=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

25.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física*
Name	*[es]*	*Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject OU:	*Prestador de Servicios de Confianza*
Subject SERIAL NUMBER:	*B99091696*
Subject CN:	*CIPSC - Subautoridad de emisión de certificados de persona física*
Subject E:	*cipsc@coloriuris.net*

X509SKI

X509 SK I	*AulqL7IF0xtj+zzAxZJqC/8tgyk=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2015-10-19T22:00:00Z*

25.2 - Service (withdrawn): Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica*
Name	*[es]*	*Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*3581065887593727996*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIfzCCBmegAwIBAgIIMbKAc5NLB/wwDQYJKoZIhvcNAQELBQAwgdsxIzAhBgkqhkiG9w0BCQEW
FGNpcHNjQGNvbG9yaXVyaXMubmV0MTgwNgYDVQQDDC9DSVBTQyAtIFJhw616IGRlIGxhIEF1dG9y
aWRhZCBkZSBDZXJ0aWZpY2FjacOzbjESMBAGA1UEBRMJQjk5MDkxNjk2MSwwKgYDVQQLDCNQcmVz
dGFkb3lgZGUgU2VydmljaW9zIGRlIENvbmZpYW56YTEYMBYGA1UECgwPQ29sb3JpdXJpcyBTLkwu
MREwDwYDVQQDHDAhaYXJhZ296YTELMAkGA1UEBhMCRVMwHhcNMTUwNzE0MTAxNTI4WhcNMjUwNzE0
MTAxNTI4WjCB8TEjMCEGCSqGSIb3DQEJARYUY2lwc2NAY29sb3JpdXJpcy5uZXQxIjBMBgNVBAMM
RUNJUFNDIC0gU3VGYXV0b3JpZGFkIGRlICAgVXpw7NuIGRlIGNlcnRpZmlj YWRvcyBkZSBwZXJz
b25hIGp1csOtZGljYTESMBAGA1UEBRMJQjk5MDkxNjk2MSwwKgYDVQQLDCNQcmVzdGFkb3lgZGUg
U2VydmljaW9zIGRlIENvbmZpYW56YTEYMBYGA1UECgwPQ29sb3JpdXJpcyBTLkwuMREwDwYDVQQH
DAhaYXJhZ296YTELMAkGA1UEBhMCRVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDO
Gdo66NCW9MtaKuU+QZqtj3vNLLzXvQ8O+GNQNNYnu9WaZt8dHBBY0flL8oIJs2w/26YrIEP4ZZdVj
SabYXoiRuXqGljV976Axp5DFd93V5MvyK8P4mojLjXlfmzh0S9nCKJdWn8vIPpvaIspgD7j6PyTT
xCOOwsuQfj2wa7H1BODcnmlxZXc5MpzruF1oiEYgb4jPUDj78xfE3tlc6tU2+WPq22kccAqRPlvd
bKv0DSjYpqtFBaSmNMNBy2s+RW+AAor2ROnDDEb9x5qZEOh/oZ+AXdiyABFElIk1x25Iy/cpZEuB
UV4UxSmNYM2OgqLGoXiadHQU2ymSgotfMQxvAgMBAAGjggMtMIIDKTB6BggrBgEFBQcBAQRuMGww
QQYIKwYBBQUHMAKGNWh0dHBzOi8vY2lwc2MuY29sb3JpdXJpcy5uZXQvY2VydGlmaWNhZG9zL2Fj
L3JhaXouY3J0MCcGCCsGAQUFBzABhhtodHRwczovL29jc3AuY29sb3JpdXJpcy5uZXQwHQYDVR0O
BBYEFDV/N48h7k8KaAB6p6JBseGVOnGuMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUcSIh
XKHznzXoDuIZrSIq+Q2caYwggEBgNVHSAEggEWMIIBEjCCAQ4GDSsGAQQBgqcnAAMBAgAwgfww
gcQGCCsGAQUFBwICMIG3Ho6i0AFMAdQBiAEEAdQB0AG8AcgBpAGQAYQBkACAAQwBJAFAAUwBDACAA
cABhAHIAYQAgAGUAbQBpAHMAaQDzAG4AIABkAGUAIABjAGUAcgB0AGkAZgBpAGMAYQBkAG8AcwAg
AHAAYQByAGEAIABzAGUAbABsAG8AIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8AIABkAGUAIABwAGUA
cgBzAG8AbgBhACAAagB1AHIA7QBkAGkAYwBhMDMGCCsGAQUFBwIBFidodHRwczovL2NpcHNjLmNv
bG9yaXVyaXMubmV0L3Bvb2l0aWNhcy8wggEIBgNVHR8EggEcMIIBGDCCAREgLqAshipodHRwczov
L2NpcHNjLmNvbG9yaXVyaXMubmV0L2NybC9hYy9hYy5jcmyigeGkgd4wgdsxIzAhBgkqhkiG9w0B
CQEWFGNpcHNjQGNvbG9yaXVyaXMubmV0MTgwNgYDVQQDDC9DSVBTQyAtIFJhw616IGRlIGxhIEF1
dG9yaWRhZCBkZSBDZXJ0aWZpY2FjacOzbjESMBAGA1UEBRMJQjk5MDkxNjk2MSwwKgYDVQQLDCNQ
cmVzdGFkb3lgZGUgU2VydmljaW9zIGRlIENvbmZpYW56YTEYMBYGA1UECgwPQ29sb3JpdXJpcyBT
LkwuMREwDwYDVQQHDAhaYXJhZ296YTELMAkGA1UEBhMCRVMwDgYDVR0PAQH/BAQDAgEGMA0GCSqG
SIb3DQEBCwUAA4ICAQDL WKUFq8Vy9UyNovIBkGA/wehyrgZI/CE2b7bqZpU/Dmrq9b2Ozj25w3DKO
tJ4pgnMth5v27800enEvms2aij6M+ajmomFkjY4h+wzeyudKJvIO/8VqKHMyf8lK YysIZ9wq9hR
2W0yKvjFhbBRmkpbwXvzzyC4wXDZrP7GuINdzYTFmVnkz8KvVgpkkd/qsL VmrpyE4rtDm7s+4coU
+s3chLGpiXthzNQD8QlPa9yBBjQ7s1Oy3fx++RqPYIVjlpt8zeqDGGSUnNl6Oodl76pPX96R/6QN
T/EVOFWnMvwP/EO8LF4kTrC/4Ov+miM4Nhk7PN0pIagZw0lkkX50Wo/ccOCbUM0/SmHW22JOG1TE
1RLwtDY0XIAEouC/aGi07DpLb9hMM1LWjn5zr3WTbARIsebYr8tu5zceORGnLdSTd4czPpe3btLbt
gZnU2NL7XgbIKycxIXtHIcQR5tcBeW9CMhSPWyAakd5w+lEfwnCT/iWMBicbcSPnh26CP15lI6
+vFvbZPjWXnW7pG7NGS4m2DqIWsjbOcZ0eRh3HZic/W8u70m9Mp3D/p5veyZa+WxriZGWco/MVK
C95l464qFJdOvvqXSQfcKYjsXBMFBCsshpwSCwo0QpjarGRns5ITg4XbN2gmq9aR048ocAx171M
JwXBq1h0V7CHFq/hzQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L: *Zaragoza*

Issuer O: *Coloriuris S.L.*

Issuer OU: *Prestador de Servicios de Confianza*

Issuer SERIAL NUMBER: *B99091696*

Issuer CN: *CIPSC - Raíz de la Autoridad de Certificación*

Issuer E: *cipsc@coloriuris.net*

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject SERIAL NUMBER: *B99091696*

Subject CN: *CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Subject E: *cipsc@coloriuris.net*

Valid from: *Tue Jul 14 12:15:28 CEST 2015*

Valid to: *Mon Jul 14 12:15:28 CEST 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CE:19:DA:3A:E8:D0:96:F4:C9:CA:69:4F:90:66:AB:63:DE:F3:4B:2E:B5:EF:43:C3:BE:18:D4:0D:35:89:EE:F5:66:99:
B7:C7:47:04:16:34:7D:F2:FC:A0:82:6C:DB:0F:F6:E9:8A:E2:10:FE:3B:65:D5:63:49:A6:D8:5E:88:91:B9:7A:86:96:35:7D:EF:A0:31:A7:90:C5:77:DD:D5:E4:CB:F2:2B:C3:F8:9A:88:CB:8D:79:5F:9B:38:74:4B:D9:C2:28:97:
56:99:CB:E5:3E:9B:DA:22:CA:60:0F:B8:F4:3F:2A:D3:C4:23:8E:C2:CB:90:7E:3D:B0:6B:B1:F5:04:E0:DC:9E:69:71:65:77:39:32:9C:EB:B8:5D:68:88:46:20:6F:88:CF:50:38:FB:F3:17:C4:DE:D9:5C:EA:D5:36:19:63:EA:DB
:69:1C:70:0A:91:3E:5B:DD:6C:AB:F4:0D:28:D8:A6:AB:45:05:A4:A6:34:C3:41:CB:6B:3E:45:6F:80:02:8A:F6:45:09:C3:0C:46:FD:C7:9A:99:10:E8:7F:A1:9F:80:5D:D8:B2:00:11:44:94:89:35:C7:6E:48:CB:F7:29:64:4B:81:5
1:5E:14:C5:29:8D:60:CD:8E:82:A2:C6:A1:78:9A:74:74:09:DB:29:BD:82:8A:DD:31:0C:6F:02:03:01:00:01

Authority Info Access	*https://cipsc.coloriuris.net/certificados/ac/raiz.crt* *https://ocsp.coloriuris.net*
Subject Key Identifier	*35:7F:37:8F:21:EE:4F:0A:68:00:7A:A7:A2:41:B1:E1:95:3A:D1:AE*
Basic Constraints	*IsCA: true*
Authority Key Identifier	*79:21:E1:5C:A1:F1:96:7C:D7:A0:36:89:66:B4:A5:AB:E4:36:71:A6*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.37799.0.3.1.2.0* *CPS text: [SubAutoridad CIPSC para emisión de certificados para sello electrónico de persona jurídica]* *CPS pointer: https://cipsc.coloriuris.net/politicas/*
CRL Distribution Points	*https://cipsc.coloriuris.net/crl/ac/ac.crl* *CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz de la Autoridad de Certificación,SERIALNUMBER=B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*2B:03:88:BB:3A:37:32:FD:55:1B:21:BE:FE:2F:6D:6C:18:D0:FC:76:20:BD:31:EC:C3:4F:71:43:7F:DE:B2:E7*

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject OU:	*Prestador de Servicios de Confianza*
Subject SERIAL NUMBER:	*B99091696*
Subject CN:	*CIPSC - Subautoridad de emisión de certificados de persona jurídica*
Subject E:	*cipsc@coloriuris.net*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2017-07-01T22:00:00Z

25.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.37799.20.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.37799.20.1.2.2*

25.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica*
Name	*[es]*	*Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject OU:	*Prestador de Servicios de Confianza*
Subject SERIAL NUMBER:	*B99091696*
Subject CN:	*CIPSC - Subautoridad de emisión de certificados de persona jurídica*
Subject E:	*cipsc@coloriuris.net*

X509SKI

X509 SK I *NX83jyHuTwpoAHqnokGx4ZU60a4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

25.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.37799.20.1.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.37799.20.1.2.2*

25.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Name *[es]* *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject SERIAL NUMBER: *B99091696*

Subject CN: *CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Subject E: *cipsc@coloriuris.net*

X509SKI

X509 SK I *NX83jyHuTwpoAHqnokGx4ZU60a4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-10-19T22:00:00Z*

25.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.37799.20.1.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.37799.20.1.2.2*

25.3 - Service (withdrawn): Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica*

Name *[es]* *Certificados Reconocidos emitidos por CA - CIPSC Emisión de certificados de persona jurídica*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *4580114715082243801*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIH0DCCBbigAwIBAgIIP4/WER8EPtkwDQYJKoZIhvcNAQELBQAwgd0xIzAhBgkqhkiG9w0BCQEW
FGNpcHNjQGNvbG9yaXVyaXMubmV0MTQwMgYDVQQDDCtDSVBTQyAtIFJhw616lCI0gQXV0b3JpZGFk
IGRlIENlcnRpZmljYWNpw7NuMRgwFgYDVQRhDA9WQVRFUy1COTkwOTE2OTYxLDAqBgNVBAsMI1By
ZXN0YWRvciBkZSBTZXJ2aWNpb3MgZGUgQ29uZmlhbnphMRgwFgYDVQQKDA9Db2xvcmI1cmIzIFMu
TC4xETAPBgNVBAcMCFphcmFnb3phMQswCQYDVQQGEwJFUzAeFw0xNTA5MTAw0DEzMjVaFw0yNTA5
MTAw0DEzMjVaMIHnMSMwIQYJKoZIhvcNAQkBFhRjaXRzY0Bjb2xvcmI1cmIzLm5ldDE+MDwGA1UE
AwwIQ0lQU0MgLSBFbWlzacOzbiBkZSBjZXJ0aWZpY2Fkb3MgZGUgcGVyc29uYSBqdXLDrWRpY2Ex
GDAWBgNVBGEMD1ZBVEVTLUI5OTA5MTY5NjEsMCoGA1UECwwjUHJlc3RhZG9yIGRlIFNlcnZpY2lv
cyBkZSBDb25maWFuemExGDAWBgNVBAoMD0NvbG9yaXVyaXMgLy5MLjERMA8GA1UEBwwIWmFyYWdv
emFxCzAJBgNVBAYTAkVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1d3NZj/sx5Ay
y55zxDM9sÃ+hennEMSNNYEPapkvDGX7p2HqBwhCD0POadn6AE+UUsjOiv4xSx7Nr11WH9tSzf61D
oPYzlDKlV1N+p8y9wmn1jqamy4BcmgTvRrFfOA6k7T1oRYE6RSAfSi5Kj1GeSSsIdy7w2TFgqBo
Qur+DptVF77H1S0IJwvEupcJcKkpPIXpCT7NrtUlz0xQ8s/x4vQ35kCbPCU12ntF3XTWVAblhPzw
x3kpRtarnZoJHF2YMNZIzKALx5bO+s9+uYsrL1INoub+2z47iRDr/nCbWpFuTW9NiygbjH8YGimIm
qFDnyB7aoibv4w0jm9QZ4gYq2wIDAQABo4HChjCCAoIwfQYIKwYBBQUHAQEEcTBvMEQGCCsGAQUF
BzAChjhodHRwczovL2NpcHNjLmNvbG9yaXVyaXMubmV0L2NlcnRpZmljYWRvcy9bYy9yYWl6LXYz
LmNydDAnBggrBgEFBQcwAYYbaHR0cHM6Ly9vY3NwLmNvbG9yaXVyaXMubmV0MB0GA1UdDgQWBBR7
ldL72ouBDQY/T4prtMmn3IyVezASBgNVHRMBAf8ECDAGAQH/AgECMB8GA1UdIwQYMBaAFFY0L T6M
9JDv34r56e9G1MUASjqMCUGCCsGAQUFBwEDBBkwFzAVBggrBgEFBQcLAjAJBgcEAIrssQECMEgG
A1UdIARBMD8wPQYEVR0gADA1MDMGCCsGAQUFBwIBFidodHRwczovL2NpcHNjLmNvbG9yaXVyaXMu
bmV0L3BvbGl0aWNhcy8wggEqBgNVHR8EggEhMIIBHTCCARmgMaAvhi1odHRwczovL2NpcHNjLmNv
bG9yaXVyaXMubmV0L2NvbC9bYy9bYy12My5jcmyygeOkgeAwgd0xIzAhBgkqhkiG9w0BCQEWFGNp
cHNjQGNvbG9yaXVyaXMubmV0MTQwMgYDVQQDDCtDSVBTQyAtIFJhw616lCI0gQXV0b3JpZGFkIGRl
IENlcnRpZmljYWNpw7NuMRgwFgYDVQRhDA9WQVRFUy1COTkwOTE2OTYxLDAqBgNVBAsMI1ByZXN0
YWRvciBkZSBTZXJ2aWNpb3MgZGUgQ29uZmlhbnphMRgwFgYDVQQKDA9Db2xvcmI1cmIzIFMuTC4x
ETAPBgNVBAcMCFphcmFnb3phMQswCQYDVQQGEwJFUzAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcN
AQELBQADggIBAMwa1CvkWcqiQybHb+oqHq0wT2gxqY1zFnicUa9+ohSvI3b0KuTFUsa4WKYXd1
b96+5EbWd+FpnOvtoP+FMBEbfyD5v7VjGsdtebE4B9eGc7TxiQ2TYMBsbjpuuQuBWHz8y3yVQiHq
hLunrcojL80BHoIolothE/7YksHSeq5SO+Qn78IVkiw1Ify+5ISYK3xoGXDIwJxjVX0PBCcGrlOTdi
NqqH6n65HCRRoq/ozyuKnqLq5C+nAziS/pmc3sqLbrjIFVTpcP1GAGWq38LWSpxSyQSPcMcxR8ME
+BHVSH+OnzmH0DbVZzDvMKbIbYgf29MwAKGT1s4wzeQIoYG7fU1mSPLPH2xTqk5LbcfkkXHJnk9K
F8GkUW/cbGV7kAuzI5x+lak5+25TGFdWbcgowtD7aBLxTvKfvsXA0Ga4fPH+QS1OsuY2mW8llEP
LUQI5QY/BxDzFTDboSRMvfS4hfNNrwXCYnf2ArnniWlbBWKdr7rz2gCEcRuNa5Qq8XBurRUw5FBT
LUQH1eDSFQE6cuaz4QOb3OnjMvkuH7q+JXi7X2ix3DNQ6UDOC+0NuZo64a7nR7Qjb+DzOQ4O1qgCf
4LCBHFw7iaSrAeFQm1lAzsRUtR8CUo+WML0AtTvkfJJfTQSialn2HV+AB2bFdAjYTzaLOthh21
RL7DkOhcUMY9

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L: *Zaragoza*

Issuer O: *Coloriuris S.L.*

Issuer OU: *Prestador de Servicios de Confianza*

Issuer 2.5.4.97: *VATES-B99091696*

Issuer CN: *CIPSC - Raíz - Autoridad de Certificación*

Issuer E: *cipsc@coloriuris.net*

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - Emisión de certificados de persona jurídica*

Subject E: *cipsc@coloriuris.net*

Valid from: *Thu Sep 10 10:13:25 CEST 2015*

Valid to: *Wed Sep 10 10:13:25 CEST 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D5:DD:CD:66:3F:EC:C7:90:32:CB:9E:73:C4:33:3D:B0:0F:A1:7A:79:C4:31:23:4D:60:43:DA:A6:4B:C3:19:7E:E9:D8:7A:81:C2:10:83:D0:F3:9A:76:7E:80:13:E5:14:B2:33:A2:BF:8C:52:C7:B3:6B:D7:55:87:F6:D4:B3:7F:AD:43:A0:F6:33:94:32:A5:57:53:7E:A7:CC:BD:C2:69:F5:8E:A6:A6:CB:80:5C:9A:04:EF:46:B1:5F:DC:E0:3A:93:B4:F5:A1:16:04:E9:14:80:7D:28:B9:2A:3D:46:79:24:9C:21:DC:BB:C3:64:C5:82:A0:68:42:EA:FE:0E:9B:55:17:BE:C7:D5:2D:08:27:0B:C4:BA:97:09:70:A9:29:3C:85:E9:09:3E:CD:AE:D5:08:CF:4C:50:F2:CF:F1:E2:F4:37:4A:40:9B:3C:25:35:DA:7B:45:DD:74:D6:54:06:C8:84:FC:F0:C7:79:29:F2:B6:AB:C5:9C:49:1C:5D:98:30:D6:48:CC:A0:0B:C7:96:CE:FB:1F:7E:B9:8B:2B:2F:57:CD:A2:E6:FE:DB:3E:3B:89:10:E2:FE:70:A1:5A:91:6E:4D:6F:4D:8B:28:21:8C:74:98:1A:69:66:A8:50:E7:C8:1E:DA:A2:26:EF:E3:0D:23:9B:D4:19:E2:06:2A:DB:02:03:01:00:01

Authority Info Access

https://cipsc.coloriuris.net/certificados/ac/raiz-v3.crt

https://ocsp.coloriuris.net

Subject Key Identifier *7B:21:D2:FB:DA:8B:81:0D:06:3F:4F:8A:6B:7C:C9:A7:DE:5C:95:7B*

Basic Constraints *IsCA: true - Path length: 2*

Authority Key Identifier *56:0E:2D:3E:8C:F4:9F:C3:BF:7E:2B:E7:A7:BD:1B:53:14:01:28:EA*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://cipsc.coloriuris.net/politicas/

CRL Distribution Points

https://cipsc.coloriuris.net/crl/ac/ac-v3.crl

CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Certificación,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *55:01:5F:B9:D2:CD:21:76:57:32:A2:34:0E:53:E4:18:4F:0C:0D:57:F7:6E:3B:4F:08:03:B6:C1:56:FF:BB:1E*

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - Emisión de certificados de persona jurídica*

Subject E: *cipsc@coloriuris.net*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

	[es]	*undefined.*

Status Starting Time *2017-07-01T22:00:00Z*

25.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.37799.20.2.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.37799.20.2.2.2*

25.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica*
Name	*[es]*	*Certificados Reconocidos emitidos por CA - CIPSC Emisión de certificados de persona jurídica*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject OU:	*Prestador de Servicios de Confianza*
Subject 2.5.4.97:	*VATES-B99091696*

Subject CN: *CIPSC - Emisión de certificados de persona jurídica*

Subject E: *cipsc@coloriuris.net*

X509SKI

X509 SK I *eyHS+9qLgQ0GP0+Ka3zJp95clXs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

25.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.37799.20.2.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.37799.20.2.2.2*

25.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica*

Name *[es]* *Certificados Reconocidos emitidos por CA - CIPSC Emisión de certificados de persona jurídica*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject OU:	*Prestador de Servicios de Confianza*
Subject 2.5.4.97:	*VATES-B99091696*
Subject CN:	*CIPSC - Emisión de certificados de persona jurídica*
Subject E:	*cipsc@coloriuris.net*

X509SKI

X509 SK I	*eyHS+9qLgQ0GP0+Ka3zJp95clXs=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2015-10-19T22:00:00Z*

25.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.37799.20.2.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.37799.20.2.2.2*

25.4 - Service (granted): Qualified timestamps issued by Coloriuris (TSACI)

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by Coloriuris (TSACI)*

Name *[es]* *Sellos de tiempo cualificados emitidos por Coloriuris (TSACI)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7213081827756070413*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIVTCCBj2gAwIBAgIIZBoDtK851g0wDQYJKoZIhvcNAQENBQAwgeMxIzAhBgkqhkiG9w0BCQEW
FGNpcHNjQGNvbG9yaXVyaXMubmY0MTowOAYDVQQDDDFDSVBTQyAtIFJlbw6J6lC0gQXV0b3JpZGFk
IGRlIFNlbGxhZG8gZGUgVGllbXBvIHYzMRgwFgYDVQRhDA9WQVRFUy1COTkwOTE2OTYxLDAqBgNV
BAsMI1ByZXN0YWRvciBkZSBTZXJ2aWNpb3MgZGUgQ29uZmlhbnphMRgwFgYDVQQKDA9Db2xvcml1
cmlzIFMuTC4xETAPBgNVBAcMCFphcmFnb3phMQswCQYDVQQGEwJFUzAeFw0xNzA3MDQxNjI3MjIa
Fw0yNzA3MDQxNjI3MjIaMIGOMTgwNgYDVQQDC90DSVBTQyAtIHYzIC0gRW1pc29yIGRlIHNlbGxv
cyBkZSB0aWVicG8gZGUgMjA0ODEYMBYGA1UEYQwPVkFURVMtQjk5MDkxNjk2MRgwFgYDVQQKDA9D
b2xvcml1cmlzIFMuTC4xETAPBgNVBAcMCFphcmFnb3phMQswCQYDVQQGEwJFUzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAK3xITrcs8QSgRl5zom6dJ787PxZAjmQN+9m1IRfXYLKfRML
bRMeOKQyHtLmhemcm/ZD39p+GkHSYiN4m2LLkgNYor9vJva3rPEcXTi6wJRzGTPRLJSUS1qrH
fY4CbJE7LOTobrfM3x/YsPxf5ALdMHkHquiASdgE06JGU5TUz3DK3tl3M7WcX/s4aSHGSkEusBfdc
xG9FRBlbqJEyf0tgoGUcay5kGJ/xddZAbX1sPcf3APn0mb74+He/IRLPXRUBf5g0FzL81Vcbl2R2
n6IzWOpnFNsNw0J38kJTSIa+s4r5bE0FswAoEzNGAF/tPUQYJPNLbfkT2dA7O4oudcCAwEAAaOC
A14wggNaMHMGCCsGAQUFBwEBBHIwcDBFBggrBgEFBQcwAoY5aHR0cHM6Ly9jaXBzYy5jb2xvcml1
cmlzLm5ldC9jZXJ0aWZpY2FKb3MvdHNhLzJhaXotdjMuY3J0MCcGCCsGAQUFBzABhhtodHRwczov
L29jc3AuY29sb3JpdXJpcy5uZXQwHQYDVR0OBBYEFGBigrcoWLbvupx7f7pzCDSBiAHLMB8GA1Ud
IwQYMBaAFGF/1LxHWP88ComvnbAq7/wCXCpaMEwGCCsGAQUFBwEDBEAwPjAVBggrBgEFBQcLAjAJ
BgcEAIvsSQECMCUGBwQAgZdcAQEMGmlkLWV0c2ktdHN0cy1FdVFDb21wbGlhbmNlMIHsBgNVHSAE
ge0wgeEwgd4GCysGAQQBgcnFAUBMHHOMIGWBggrBgEFBQcCAjCBiR6BhgBDAGUAcgBlAGkAZgBp
AGMAYQBkAG8AIABjAHUAYQBsAGkAZgBpAGMAYQBkAG8AIABkAGUAIABlAG0AaQBzAGkA8wBuACAA
ZABlACAAcwBlAGwAbABvAHMAIABkAGUAIAB0AGkAZQBtAHAAbwAgAGUAbABlAGMAdAByAPMAbgBp
AGMAbwBzMDMGCCsGAQUFBwIBFidodHRwczovL2NpcHNjLmNvbG9yaXVyaXMubmV0L3BvbGl0aWNh
cy8wggEcBgNVHR8EggEaMIIBJDCCASCgMgAwhi5odHRwOi8vY2lwc2MuY29sb3JpdXJpcy5uZXQv
Y3JsL3RzYS90c2EtdjMuY3JsooHppIHmMHjMSMwJQYJKoZIhvcNAQkBFhRjaXBzY0Bjb2xvcml1
cmlzLm5ldDE6MDgGA1UEAwwxQ0lQU0MgLSBSYcOteiAtIEF1dG9yaWRhZCBkZSBTZWxsYWRvIGR1
IFRpZW1wbyB2MzEYMBYGA1UEYQwPVkFURVMtQjk5MDkxNjk2MSwwKgYDVQQLDCNQcmVzdGFkb3Ig
ZGUgU2VvdmIjaW9zIGRlIENvbmZpYW56YTEYMBYGA1UECgwPQ29sb3JpdXJpcyBTLkwuMREwDwYD
VQQHDAhaYXJhZ29YTELMAkGA1UEBhMCRVMwDgYDVR0PAQH/BAQDAgbAMBYGA1UdJQEB/wQMMAoG
CCsGAQUFBwMIMA0GCSqGSIb3DQEBDQUAA4ICAQCpGU+Tl7nZqHXopoa0hN2pzvN6a2m3AtN9UGWZ
2oFsXD+HDL15OMIy5yAQYloa2tFSGnI11UG9N+T3/7FALNh3n29nFWbaQ6+amFKB/qcp+xIwyTvPy
CkbRhdIM/nNu1+MlImuKp06dXCelEpnujIQ0Kan72sCwJNUaQMXifoN7LWCfZ8BdGzezTXuaCP
I11BZEB6xAd8OwDar1/BEGkH01iSNlbec107bC/7StPQf6ALJ7YLMqPKZMAVTXi33sJ38bh32c2n
kTGxjdwaZzBoVAPj9nGg6jyRk951FFYtzp+YVFEbDMT+S/maTw/MBmRGXtCDk4gXWmFfKkzUjctx
hqESEilNvP0ajV7NwLDE4dgpVnvqG6GUFarATnmtpYHMCz3smB0a/udhfxrWHT3Iv8SiQ/EGq4Rc
VuYE7k2z5xaBHles3rnNf4R560lDaGzAHeh/hfIvfVTLKnWzoeCu6xpHjxBBkUee14q+S6P+ynR60
cT0w8z6Suf4nkP9IibPN68Kq2FvUYMSyYXqfo/E88AZApwAu4Ia9nnSYBITesG3ljxRPJEOJPAth
sXHb4InD5D5bbMKfa6ri5Kq12nfMydRlChlXCEQLzxgs0lBl4REfI23cXXf9L12l8cl3veiE6Cbcn
AkjoDJca1/6gwrbG4IB1XFOEGLtg03duVhMz+A==

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer L: *Zaragoza*

Issuer O: *Coloriuris S.L.*

Issuer OU: *Prestador de Servicios de Confianza*

Issuer 2.5.4.97: *VATES-B99091696*

Issuer CN: *CIPSC - Raíz - Autoridad de Sellado de Tiempo v3*

Issuer E: *cipsc@coloriuris.net*

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - v3 - Emisor de sellos de tiempo de 2048*

Valid from: *Tue Jul 04 18:27:29 CEST 2017*

Valid to: *Sun Jul 04 18:27:29 CEST 2027*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AD:F1:21:3A:DC:B3:C4:12:81:19:79:CE:89:BA:74:9E:FC:EC:FC:99:02:39:90:37:EF:66:D6:54:5F:5D:82:CA:7D:13:0B:6D:13:1C:38:64:32:1E:D2:E7:B6:17:A6:72:6F:D9:0F:7F:69:F8:68:8C:49:87:CD:E2:6D:8B:2E:48:0D:62:8A:FD:C5:F2:2F:6B:7A:CF:11:E5:D3:93:AC:09:45:E1:93:3D:12:C9:E5:44:B5:AA:2A:C7:7D:8E:02:6C:91:3B:2C:E4:E8:6E:B7:CC:DF:1F:D8:B0:FC:5F:E4:02:DD:30:79:07:AA:E8:80:49:D8:03:EA:31:94:E5:35:33:DC:32:B7:B6:5D:CC:ED:67:17:FE:CE:1A:48:71:92:90:4B:AC:05:F7:5C:C4:6F:45:44:12:1B:A8:91:32:7F:4B:60:A0:65:1E:6B:2E:64:18:9F:F1:75:D6:40:6D:7D:6C:3D:C7:F7:00:F9:F4:99:BE:F8:F8:77:BF:21:12:CF:5D:15:01:7F:18:34:17:32:FC:D5:57:21:27:64:76:9F:A2:33:58:EA:67:14:DB:0D:C3:42:77:F2:42:53:48:86:BE:B3:8A:F9:6C:4D:05:B3:00:28:13:33:46:00:5F:ED:3D:44:18:24:F3:4B:6D:F7:E4:4F:67:40:4F:4E:28:B9:D7:02:03:01:00:01*

Authority Info Access

https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt

https://ocsp.coloriuris.net

Subject Key Identifier *60:62:82:B7:28:58:B6:EF:BA:9C:7B:7F:BA:73:08:34:81:88:01:CB*

Authority Key Identifier *67:FF:D4:BC:47:58:FF:3C:0A:89:AF:9D:B0:2A:EF:FC:02:5C:2A:5A*

Certificate Policies

Policy OID: 1.3.6.1.4.1.37799.20.5.1

CPS text: [Certificado cualificado de emisión de sellos de tiempo electrónicos]

CPS pointer: https://cipsc.coloriuris.net/politicas/

CRL Distribution Points

http://cipsc.coloriuris.net/crl/tsa/tsa-v3.crl

CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Sellado de Tiempo v3,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D8:9C:1C:4E:94:77:B4:76:8B:1C:46:F7:E1:61:29:54:1C:CD:E1:99:51:A4:91:2A:F6:57:43:E7:BD:55:13:BE*

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - v3 - Emisor de sellos de tiempo de 2048*

X509SKI

X509 SK I *YGKCtyhYtu+6nHt/unMINIGIAcs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time *2017-09-27T10:00:00Z*

25.5 - Service (granted): Qualified timestamps issued by Coloriuris (TSACI) v3.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by Coloriuris (TSACI) v3.1*

Name *[es]* *Sellos de tiempo cualificados emitidos por Coloriuris (TSACI) v3.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7842311533657933281*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIVzCCBj+gAwIBAgIIbNV8yh2hReEwDQYJKoZIhvcNAQENBQAwgeUxIzAhBgkqhkiG9w0BCQEW
FGNpcHNjQGNvbG9yaXVyaXMubmV0MTwwOgYDVQQDDDNDSVBTQyAtIFJhw616lC0gQXV0b3JpZGFk
IGRlIFNlbGxhZG8gZGUgVGllbXBvIHYzLjExGDAWBgNVBGEMD1ZBVEVTLUlSOTA5MTYSNjEsMCoG
A1UECwwjUHJlc3RhZG9yIGRlIFNlcnZpY2lvcyBkZSBDb25maWFuemExGDAWBgNVBAoMD0NvbG9y
aXVyaXMgUy5MLjERMA8GA1UEBwwIWmFyYWdvemExCzAJBgNVBAYTAkVTMB4XDTE4MDQwNjExMzUz
NVoXDTI4MDQ0uNTExMzUzNVowgaoxVDBSBgNVBAMMS0NUIFNDIC0gdjMuMSAtIEVtaXNvciBkZSBz
ZWxsb3MgZWxlY3Ryb25pY29zIGNlYWxpZmljYWRvcyBkZSB0aWVtcG8gZGUgMjA0ODEYMBYGA1UE
YQwPVkFURVMtQjk5MDkxNjk2MRgwFgYDVQQKDA9Db2xvcmlIcmlzIFMuTC4xETAPBgNVBAcMCFph
cmFnb3phMQswCQYDVQQGEwJFUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMTAmp+m
SnfQBM7HGuq8oz3qek8KAamydoYGUgGDMIsuKHnNyt0O1DsPpm+tFpc/FfIMLVrZcHRamvlKOm
ADCm634rPU4muEXxMbwxyFWDSb0I+O3SvrHIPa7OxPp+PxnCpHX0H0FinUv4zSZl1qMvVBKdMY1Y
SHBeSLMGmBoRrSlbA9vO6fOlpJrx+0dZsUnE7XLNRotBhSO6XmYdLcgeCtOzgBlMbaD3txRxTpV6
lRE8DK9lRem1o4h79UUXKn7NrqhJIQfwrlhnq/ZqZc5NIf/YhRRTWTU0e1O0c/9s08VGwjNaVQ0a
TVkc6b7qHdHN0WKuTk2JtRxf5zfe/wEiCAwEAAaOCA0IwggM+MB8GA1UdIwQYMBaAFBG8NTz17BMm
DmBDtfiGqf54dJwFqMIGCBggrBgEFBQcBAQR2MHQwRwYIKwYBBQUHMAKGO2h0dHBzOi8vY2lwc2Mu
Y29sb3JpdXJpcy5uZXQvY2VydGlmaWNhZG9zL3RzYS9yYWl6LXYzLjEuY3J0MCkGCCsGAQUFBzAB
hh1odHRwczovL29jc3B2My5jb2xvcmI1cmlzLm5ldDCB7gYDVR0gBIHmMIHjMIHgBgsrBgEEAYKn
JxQFATCB0DAzBggrBgEFBQcCARYnaHR0cHM6Ly9aXBzYy5jb2xvcmI1cmlzLm5ldC9wb2xpdGlj
YXMvMGYBggrBgEFBQcCAjCBnx6BiABDAGUAcgB0AGkAZgBpAGMAYQBkAG8AIABlAGUAIABlAG0A
aQBzAGkA8wBuACAAZABlACAAcwBlAGwAbABvAHMAIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8AcwAg
AGMAdQBhAGwAaQBmAGkAYwBhAGQAbwBzACAAZABlACAAdABpAGUAbQBwAG8wFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwgwJQYIKwYBBQUHAQMEGTAXMBUGCCsGAQUFBwsCMAkGBwQA+xJAQIwggE1BgNV
HR8EggEsMIIBKDCCASSgNKAyhjBodHRwOi8vY2lwc2Mu Y29sb3JpdXJpcy5uZXQvY3JsL3RzYS90
c2EtdjMuMS5jcmyigeukgegwgeUxIzAhBgkqhkiG9w0BCQEWFGNpcHNjQGNvbG9yaXVyaXMubmV0
MTwwOgYDVQQDDDNDSVBTQyAtIFJhw616lC0gQXV0b3JpZGFkIGRlIFNlbGxhZG8gZGUgVGllbXBv
IHYzLjExGDAWBgNVBGEMD1ZBVEVTLUlSOTA5MTY5NjEsMCoGA1UECwwjUHJlc3RhZG9yIGRlIFNl
cnZpY2lvcyBkZSBDb25maWFuemExGDAWBgNVBAoMD0NvbG9yaXVyaXMgUy5MLjERMA8GA1UEBwwI
WmFyYWdvemExCzAJBgNVBAYTAkVTMB0GA1UdDgQWBBR+Wtse7S4TtYlQrF7CPVSqeyOCrDAOBgNV
HQ8BAf8EBAMCBsAwDQYJKoZIhvcNAQENBQADggIBABqPSZHYppcPef TPHCiK5YiYH5TxAj+Omr2K
NpqodEvHFE7q5WorwoAFtNwFb8YzVdzx7nb+87yf/MJglc1D/lNVJoQLtc2FAW3GDGKygzS3o4D8
XA68j7UESMtYar3/m05va6Rdz5+EuxTQIg9bbCxx20smMVLSiSNNuIbxEc3YDvkJjbcV07d
uPTndqcoCk/G+hhSsfS9c18snBy16EADIMGIaUyXQffoJlvkP3RzvOwU6LmPJqyWrjgkRemwS7wE
Jr5RMT/xH+J0g034lRPZRZ/3wDf/gDpQwwAp3BU1r27vaR9OC1qMlhilcxPwhIfiFciU6QL5P9c
hIHveL05bTh8Ch+UlD5IW0vZTqKkgzrqXqXNVhtGH9Ant+17o/hKjujOSn7JAUZ7yIR4/8ZnocM
7y4HdLuRj++xZsRJiLqoeNzzWYA+T+CVIHT0oOKFuowKnNWUP0FNcxaYqzYrY268EI9yv2XRXdk
Vm7nKMe9ITsxr8ILswt6ztc2arEBJCRNPvK66E/vTVLRUu6/GzOMGt9KInubsfe94ZIk9Bb7IU/QS
01mGd/qDNdSNSKhDmZ+V3B84qdepev1sJa+I5VJb25pk8XgMXgX03+oNqsU/6nuhlOBzEU3dIqfiE
K8t1HGJWqYWOB6zanK+B24fZXyGeCe+I1kUsr9ma

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer L: *Zaragoza*

Issuer O: *Coloriuris S.L.*

Issuer OU: *Prestador de Servicios de Confianza*

Issuer 2.5.4.97:	*VATES-B99091696*
Issuer CN:	*CIPSC - Raíz - Autoridad de Sellado de Tiempo v3.1*
Issuer E:	*cipsc@coloriuris.net*
Subject C:	*ES*
Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject 2.5.4.97:	*VATES-B99091696*
Subject CN:	*CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048*
Valid from:	*Fri Apr 06 13:35:35 CEST 2018*
Valid to:	*Wed Apr 05 13:35:35 CEST 2028*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C4:C0:9A:9F:A6:4A:77:EB:40:13:3B:1C:68:AA:F2:8C:F7:A9:E9:3C:28:06:A6:8D:DB:98:19:48:E0:18:33:25:B2:E2:87:9C:DC:B4:3B:50:EC:3E:99:BE:89:F1:69:7B:F1:5D:7C:C2:D5:FD:97:07:46:E9:F2:94:A3:A6:00:30:A6:EB:7E:2B:3D:4E:26:B8:45:F1:31:BC:31:C8:55:83:4A:1D:08:F8:ED:D2:BE:B1:C8:3D:AE:CE:C4:FA:7E:3F:19:C2:A4:75:F4:1F:41:62:9D:4B:F8:CD:26:65:D6:A3:2F:54:12:9D:31:8B:58:48:70:5E:48:B3:06:98:1A:11:AD:22:1B:03:DB:CE:E9:F3:A5:A4:9A:F1:FB:47:59:B1:49:C4:ED:72:CD:46:8B:41:85:23:BA:5E:66:1D:2D:C8:1E:0A:D3:B3:80:19:4C:6D:A0:F7:B7:14:71:4E:95:7A:95:11:3C:0C:AF:65:45:E9:B5:A3:88:7B:F5:45:17:2A:7E:CD:AE:A8:49:21:07:F0:AE:58:67:AB:F6:6A:65:CE:4D:21:FF:D8:85:14:53:59:35:34:7B:53:B4:73:FF:6C:D3:C5:46:C2:33:5A:55:08:5A:4D:59:1C:E9:BE:EA:1D:D1:CD:D1:62:AE:4E:4D:89:89:1C:5F:E7:37:DE:FF:01:02:03:01:00:01*
Authority Key Identifier	*11:BC:35:3C:F5:EC:13:26:0E:60:43:B5:F8:86:A8:4E:1D:27:01:6A*
Authority Info Access	*https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt* *https://ocspv3.coloriuris.net*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.37799.20.5.1* *CPS pointer: https://cipsc.coloriuris.net/politicas/* *CPS text: [Certificado de emisión de sellos electrónicos cualificados de tiempo]*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl* *CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Sellado de Tiempo v3.1,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES*
Subject Key Identifier	*7E:5A:DB:1E:ED:2E:13:B5:89:50:AC:5E:C2:3D:54:AA:7B:23:82:AC*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*6C:17:A0:5F:0C:77:B9:6A:B0:39:A3:F8:50:58:73:1E:EB:02:F5:2F:B6:6D:87:D1:9B:93:D2:27:8D:82:64:99*

X509SubjectName

Subject C:	*ES*

Subject L:	*Zaragoza*
Subject O:	*Coloriuris S.L.*
Subject 2.5.4.97:	*VATES-B99091696*
Subject CN:	*CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048*

X509SKI

X509 SK I	*flrbHu0uE7WJUKxewj1Uqnsjgqw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-05-24T00:00:00Z

26 - TSP: UANATACA, S.A

.

TSP Name

Name	*[en]*	*UANATACA, S.A*
Name	*[es]*	*UANATACA, S.A*

TSP Trade Name

Name	*[en]*	*UANATACA*
Name	*[es]*	*UANATACA*
Name	*[en]*	*UANATACA S.A.*
Name	*[en]*	*VATES-A66721499*

PostalAddress

Street Address	*[en]*	*Riera de Can Todà, 24-26,6º-1ª*
Locality	*[en]*	*Barcelona*
State Or Province	*[en]*	*Barcelona*
Postal Code	*[en]*	*08024*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Riera de Can Todà, 24-26,6º-1ª*
Locality	*[es]*	*Barcelona*
State Or Province	*[es]*	*Barcelona*
Postal Code	*[es]*	*08024*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:info@uanataca.com*
URI	*[en]*	*http://www.uanataca.com*

TSP Information URI

URI	*[en]*	*http://www.uanataca.com*
URI	*[es]*	*http://www.uanataca.com*

26.1 - Service (granted): Qualified Certificates issued by UANATACA CA1 2016

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by UANATACA CA1 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por UANATACA CA1 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6611671282825056795*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIWjCCBkKgAwIBAgIIW8FgADhwUhswDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHUlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRswGQYDVQQDDBlVQUFBVEFDQSBSb290IDIwMTYxGDAWBgNVBGEMDUZBVEVTLUE2NjcyMTQ5OTAe
Fw0xNjAzMTExMDM1MzNaFw0yOTAzMTExMDM1MzNaMIG4MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7
QmFyY2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20vYWRkcmVz
cykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUCl VQU5BVEFDQTEaMBgGA1UE
AwwRVUFOQVRBQ0EgQ0ExIDIwMTYxGDAWBgNVBGEMDUZBVEVTLUE2NjcyMTQ5OTCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAN/92IPM78xJtmGkLZ8xG7CEHN9Orwb6xzD3wBGaWBW4b
wIoJHw9vgEBdY4a/yLnI33kgh+mJIry8DcYmbkUx+/9m9AbINR/W4QW90LOvCf168R5v3BifIkKR
jLNbzG81Vo4AuU12NkWTvBq/8vNURcK8H4/TcxxqstDVA7aNzRoj2zmTLPQ0Ct0OTIur/zZb+vf1
iZ/vQUUbCsAB2x5udnp0awml/DutwUoas+28cGHi1zpT2OFOuAg5HTjrcqCSDi5x4h5+r99oIr
+V34TAIO0aCICRGS2/uTdI0bcXduraaV0/Q6K7Rvvwk2NEyXSCS3IMLVVXYH49UhqRB+36uPNDdJ
cQUkBP+G/t0XMVDNIwOZHGiA0yfUSogPScdFyWYJICt58JJkJXp2ANWYmdZvQKJQ8aUdceEoc60G
A0763jD+q4hZAVww7J41Dsu9DNN4ziPurz0kZx3f8fjO0Io+uYPcty/BbHjRytWZ0DoIIj915Xw1
glqHYZFBcLH9BOhVGebmeaaGZy/hwbTfTSoaRGIHge3lZwsIkys0yDZW4ETdNWR4DnKm9gNM0PGim
5v6nI/lqA8Ygpowyow3LWYIa1Gf9C1THLxj/ausZcbf7NWIGNgS9Rw9mDyi/gtbzaVy9HuNXtVLkl
VfhYJbDOev7kSsNJJ8Fct8BTgNxzAgMBAAGjggJjMIICXzB+BggrBgEFBQcBAQRyMHAwNgYIKwYB
BQUHMAGGKmh0dHA6Ly9vY3NwMS51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzA2BggrBgEF
BQcwAYYgaHR0cDovL29jc3AyLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AvMB0GA1UdDgQW
BBQice+wY3/1ecTDIkR/RBAwqI/9N5TASBgNVHRMBAf8EECDAGAQH/AgEAMB8GA1UdIwQYMBaAFFUs
8byhXmuoC+lVxBb/Jb3kZosMBwGA1UdEgQVMBOBEWluZm9AdWFuYXRhY2EuY29tMIHMBgNVHSAE
gcQwgcEwgb4GBFUdIAAwgbUwMwYIKwYBBQUHAgEWJ2h0dHA6Ly93d3cudWFuYXRhY2EuY29tL3B1
YmxpYy9wa2kvZHBjLzB+BggrBgEFBQcCAjByDHBDZXJ0aWZpY2FkbyBkZSBsYSBFbmRpZGFkIGRl
IENlbnRpZmlpYWNpw7NuIHN1YmVyZGluYWRhIGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGljL3BraS9kcGMvMIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh0dHA6Ly9j
cmwxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9hcmxfdWFuYXRhY2EuY3JsMD6gPKA6hjho
dHRwOi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvYXJsX3VhbmF0YWNhLmNybDAO
BgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAAojxg3aMg09U/WtnppWXninAOWn+Zfr
eHxz7kp1uuI02xnqbgzLKcwJ2xiHrIAgGxX2nLjXQ7PrWcUAXJ87KJKU7HOwVyDapLTcGcOs1
yxky12LH6kryjG6l/Ulqrqk9nPQxjBhSmAGOPCfmhtRYR2bTGJjN9JSUVT//ZbbF7BhQgPu+jChW
46VrR7ztCSFQEdHwS65MUc8imXGxTySQ1grecnK06MIX3I9srFtpWoGuXVs5r4JFEnZjARTCDiRH
DzxjM9B7OevvhGvVV/oMgxaj0TPwM3IB6i5FNrweg+XQeGNcaXvo8RLvJld0dx+3KKX0IDthqLiqx
z/tG99MsauzfI1l/8QJBpWuKdtCsEWw/4PZAFZhdWB4Yi8EFwX2ICIdJ1J1vnWbTfMS5N948BcOM0
6dSyZBTPXqJx3AuFTYZtAWzpwSZ3jAEU5ugdTnyapvJ3IXtKNEsV5ofmBAqmgziTYzSIn7H+U+Qi
/5mehgaVho35xiSiuMsO6/8eY12rwdehf+GL+G9Krc6eURXAbtUPAsl0nICKNuqWZCKM1Kt59oy6
xtJFa+nfGDejc7oOkxi39tHZ2hk28szEgQCoQhzPz1ws0gUcIVXpx4N8o7GsrASRyt7MZW1nm42s
5S91gKJvoXW63WMIFly6cTXzHUCIOC1QjKOyWO9z9W
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA ROOT 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-A66721499*
Subject CN:	*UANATACA CA1 2016*
Subject OU:	*TSP-UANATACA*
Subject O:	*UANATACA S.A.*
Subject L:	*Barcelona (see current address at www.uanataca.com/address)*
Subject C:	*ES*
Valid from:	*Fri Mar 11 11:35:33 CET 2016*
Valid to:	*Sun Mar 11 11:35:33 CET 2029*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DF:FD:D8:93:CC:EF:C8:B1:26:D9:E7:1A:42:D9:F3:11:BB:08:41:CD:F4:E8:AB:C1:B1:71:CC:3F:F0:04:66:96:05:6E:1B:C2:5A:09:1F:0F:6F:80:40:5D:63:86:BF:C8:B9:C8:DF:79:20:87:F9:89:22:BC:BC:0D:C6:26:6E:45:31:FB:FF:66:F4:06:C8:35:1F:D6:E1:05:BD:D0:B3:AF:09:FD:7A:F1:1E:6F:DC:17:FC:22:42:91:8C:B3:5B:CC:6F:35:56:8E:00:B9:42:36:36:45:93:BC:1A:BF:F2:F3:54:45:E2:BC:1F:8F:D3:7B:1C:6A:B2:D0:D5:03:B6:8D:CD:1A:23:DB:39:93:2C:F4:34:0A:DD:0E:4C:8B:AB:FF:36:5B:FA:F7:F5:89:9F:EF:41:45:1B:0A:C0:01:DB:1E:6E:76:7A:74:6B:09:A5:FC:3B:AD:C1:4A:1A:B3:ED:BC:70:61:E2:D7:3A:53:D8:E1:4E:B8:08:39:1D:38:EB:8D:EA:82:F0:38:9F:E7:1E:21:E7:EA:FD:F6:82:1F:F9:5D:F8:4C:02:0E:D1:A0:A2:09:11:92:DB:FB:93:74:8D:1B:71:77:6E:AD:AB:95:D3:F4:3A:2B:B4:62:BF:09:36:34:4C:97:E4:24:B7:7C:C2:FD:55:76:07:E3:D5:21:A9:10:7E:DF:AB:8F:34:37:49:71:05:24:04:FF:86:FE:DD:17:31:50:CD:23:03:99:1C:68:80:D3:27:D4:4A:88:0F:49:C7:45:C9:66:09:94:2B:79:F0:92:64:25:7A:76:00:D5:98:99:D6:6F:40:A2:10:F1:A5:1D:79:E1:28:73:AD:06:03:4E:FA:DE:30:FE:AB:88:59:01:5C:30:EC:9E:35:0E:CB:BD:0C:D3:78:CE:23:EE:AF:3D:24:67:1D:DF:F1:F8:CE:D0:8A:3E:B9:83:DC:B7:2F:C1:6C:78:D1:CA:D5:99:D0:3A:08:22:3F:48:E5:7C:35:82:5A:87:61:91:41:70:B1:FD:04:E8:55:19:E6:E6:79:A6:86:67:2F:E1:C1:B4:DF:4D:2A:1A:44:62:07:81:ED:E5:67:0B:3F:93:2B:34:C8:36:56:E0:44:DD:35:64:78:0E:72:A6:F6:03:4C:D0:F1:A6:E6:FE:A7:52:DA:80:F1:88:29:A3:0C:A8:C3:72:D6:60:86:B5:1A:5F:46:4C:7B:4B:BE:3F:EE:B1:97:1B:23:B3:56:20:63:60:4B:D4:70:F6:D9:83:CA:2F:E0:B5:BC:EE:57:2F:47:B8:D5:ED:54:B9:25:55:F8:58:25:B0:CE:7A:FE:E4:4A:C3:49:27:C1:5C:B7:C0:53:80:DC:73:02:03:01:00:01*
Authority Info Access	*http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*
Issuer Alternative Name	*info@uanataca.com*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.uanataca.com/public/pki/dpc/* *CPS text: [Certificado de la Entidad de Certificación subordinada de UANATACA. Ver http://www.uanataca.com/public/pki/dpc/]*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl* *http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*35:A9:92:84:A2:20:78:9B:A0:E0:62:EE:FF:1B:5F:2F:74:BE:43:75:44:69:97:7C:B3:18:C7:C8:6A:D4:8F:9F*

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2019-10-28T01:00:00Z*

26.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

26.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.2.6.2*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.3.6*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.4.6.2*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.7.6*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.8.6*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.9.6*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.11.6*
Description		

26.1.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by UANATACA CA1 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por UANATACA CA1 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97:	*VATES-A66721499*
Subject CN:	*UANATACA CA1 2016*
Subject OU:	*TSP-UANATACA*
Subject O:	*UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

X509SKI

X509 SK I *LXHvsGN/9f3ggyJEf0QQMIFPTeU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-06-24T00:00:00Z*

26.1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.1.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

26.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.2.6.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.3.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.4.6.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.7.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.8.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.9.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.11.6*

Description

26.1.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by UANATACA CA1 2016*

Name *[es]* *Certificados Reconocidos emitidos por UANATACA CA1 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

X509SKI

X509 SK I *LXHvsGN/9f3ggyJEf0QQMIFPTeU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-02-15T01:00:00Z*

26.1.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.1.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

26.1.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.2.6.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.3.6*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.4.6.2*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.7.6*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.8.6*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47286.1.9.6*
Description		

26.1.6 - History instance n.3 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by UANATACA CA1 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por UANATACA CA1 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97:	*VATES-A66721499*
Subject CN:	*UANATACA CA1 2016*
Subject OU:	*TSP-UANATACA*
Subject O:	*UANATACA S.A.*
Subject L:	*Barcelona (see current address at www.uanataca.com/address)*
Subject C:	*ES*

X509SKI

X509 SK I	*LXHvsGN/9f3ggyJEf0QQMIFPTeU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

26.1.6.7 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.3.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.3.2*

26.1.6.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.1.7 - History instance n.4 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by UANATACA CA1 2016*

Name *[es]* *Certificados Reconocidos emitidos por UANATACA CA1 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

X509SKI

X509 SK I *LXHvsGN/9f3ggyJEf0QQMIFPTeU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-14T22:00:00Z*

26.1.7.9 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.3.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47286.1.3.2*

26.2 - Service (granted): Qualified Certificates issued by UANATACA CA2 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by UANATACA CA2 2016*

Name *[es]* *Certificados Cualificados emitidos por UANATACA CA2 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2317042835735686419*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIWjCCBkKgAwIBAgIIICfKLtFjrRMwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmFgKHNlZSBidXlyZWS0lGFkZHIlc3MgYXQgd3dLnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUys5BLjEYMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRswGQYDVQQDDBJVQU5BVEFDQSBST09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAe
Fw0xNjAzMTExMDM3MzFaFw0yOTAzMTExMDM3MzFaMIG4MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7
QmFyY2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzKGF0IHd3dy51YW5hdGFjYS5jb20vYWRkcmVz
cyksIjAUBgNVBAoMDVVBTkFUQUNBIFMuQSAxFTATBgNVBAsMDFRTUCIVQU5BVEFDQTEaMBgGA1UE
AwwRVUFOQVRBQ0EgQ0EyIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAM9kwiDGaY0Sgs8VgEawD+YBhye+CX3RH9S+MOdgDGRNqpN
UzEDEwChjTBMV6cx+1u8gvtn+H4ITaCGkea6nLIAN6iEaVV5SPmBt9KApR6wTlbCljs5yJPNZ55S
g/FGYHruQLZ3D3stIrnKbTamB2sGkWGruPzyIUyOeBO1Tc0A92YvXdA0I0SRJy9Fjslbbeeqt
WTVI5Rk8Tx6ym5BDC7gp27stfCP9K/WECxjFIMqdHtm+bdSyyYTm+seSC4razZ+9fiSEBmRvbpPd
EtZug38UoSr/Yp3bo9c09qLO6N35JO0pcSjG5/UEZyC9wXSzRFpq7FY2lX2l0yZpbc553QyTbRul
TGzQENjy3J5YaAd6BtV0oEa/TRjtBsbbIc3e7LFcFHNCx9A0n+LoTUyj04B7A7tzAMkwfM5VFNF
ImtkWJgTbQLzVZtnqmm/Fmf40LynMV5XmdBqS5v0dtmdDrIcuNpY8m4AQOEdgzTaGwLityMWMepN
EKN1Paw0I1P4HanSRbkI5K56sAcFVseuA6QVJGHQ+rdSv8nCFAF+pLd3rI7VmaQna0wkJvSEIa5h
2CDGesXr39VvBuQONDb/nM/acBOjpOtmwsVCi8hRmPKvRvzcqpUmJlWhUMBtHr0Rcw7+bOP92sNA
tEsfOOdxD+3WNuAufGaEizzR1XdZAgMBAAGjggIjMIICXzB+BggrBgEFBQcBAQRyMHAwNgYIKwYB
BQUHMAGGKmhldHA6L y9vY3NwMS1YW5hdGFjYS5jb20vcHVibGlpL3BraS9vY3NwLzA2BggrBgEF
BQcwAYYqaHR0cDovL29jc3AyLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AvMB0GA1UdDgQW
BBR9V+dgc84HRqnio2jw4RGydJIz/TASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFFUs
8byhXrmuoC+JVxBb/Jb3kZosMBwGA1UdEgQVMBOBEWluZm9AdWFuYXRhY2EuY29tMHMBgNVHSAE
geQwgeEwgb4GBFUdIAAwgbUwMwYIKwYBBQUIAgEWZ2hldHA6L y93d3cudWFuYXRhY2EuY29tL3B1
YmxpY y9wa2kvZHBjLzB+BggrBgEFBQcCAjByDHBDZXl0aW2pY2FkbyBkZSBsY SBFbnRpZGFkIGRl
IENlcnRpZmljYWNpw7NuIHN1Ym9yZGluYWRhIGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGlpL3BraS9kcGMvMIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh0dHA6L y9j
cmwxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NvbC9hcmxfdWFuYXRhY2EuY3JsMD6gPKA6hjho
dHRwOi8vY3JsMS1YW5hdGFjYS5jb20vcHVibGlpL3BraS9qcmwvYXJsX3Vhbmf0YWNhLmNvbDAO
BgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAAcY0dMxU6W7K6TKoAIfO41WGYj/dIeB
FBN7Y6f72KhP5o6cdRmvLauANdEn5HO5P04mkf7T140bR57vybM1b4NTTGndBqogXrjmZLC8DO3F
m6XhXo4Qwdbe9c+0P3eiWvgyruv0nisJGWQW5/mViK/hJbw6RnU925STlF47XtqDqcS1wXJImSy
U/65hYCnfiwgIA2B/olP0VkbYRrQfZhTMfC8fQW+f3G11+TDeEcJkXaduJ/GCCvGt1KcgEi0LaeV
1T7z9wjfKO21PFeTuZFiVPW167NSKsJpwGhG8A4VrjrJJS4lIPAzHLIBiG5ho/ibcK7QDAXOG2PM
JBr38Tv1TzsWZTim4XVTbsLzzHaXRlmj5ZLXagyVriJadZIYQdrJbdMdlJ+gthQAqmt7mctVFjMB
FhNybQzvfcfJwYrYnOCE7BdWaauKLHT3DR+gQYjncwD5p4Gq9Y3GFLGO1q9LQiSdYzCKrRx4uNnM
QbZAAKnFGauSci0029bme+1DSN+gYjd1vDLXh1LzIFyxs76DbZZmZXacGyKj+E+gSw190pInXfZ
+IQcPn/9qvdSOPgrLQGm7AWQSbbIK1yWnXHz7a0WVfK3rELSSvVbtd5mdf8QF2tgq59/uMzJ0CT
nxMVK+0fx83luCN81YLsUpdpc3e0URG7eDMKNG54WvtW

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA ROOT 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA2 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

Valid from: *Fri Mar 11 11:37:31 CET 2016*

Valid to: *Sun Mar 11 11:37:31 CET 2029*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CF:64:C2:20:C6:69:8D:12:82:CF:15:80:46:B0:7C:9F:98:06:1C:9E:F8:25:F7:44:7F:52:F8:C3:9D:80:31:91:36:AA:4D:
53:31:03:13:00:A1:8D:30:4C:57:A7:31:FB:5B:BC:82:F9:FE:1F:8D:65:4D:A0:86:91:E6:BA:9C:B2:00:37:A1:08:69:55:79:48:F9:81:B7:D2:80:A5:1E:B0:4E:56:C2:96:3C:79:C8:93:CD:67:9E:52:83:F1:46:60:7A:EE:40:B6:77:0
F:7B:2D:D6:DA:F8:2A:1F:D3:BA:6F:36:FE:C1:A4:5B:6A:EE:3F:3C:A5:52:DC:8E:78:13:93:73:40:3D:D9:8B:F7:19:D0:34:D1:24:49:CB:D1:63:B2:56:DB:A1:EA:AD:59:35:48:E5:19:3C:4F:17:F2:9F:90:43:0B:B8:29:DB:BB
:2D:7C:23:FD:2B:F5:84:0B:18:C5:20:CA:9D:1E:D9:BE:6D:D4:B2:C9:84:E6:FA:C7:92:0B:8A:DA:CD:9F:BD:7D:24:84:06:64:6F:6E:93:DD:12:D6:6E:83:7F:14:A1:2A:FF:62:9D:DB:A3:D7:34:F6:A2:CE:E8:DD:F9:24:ED:2
9:71:28:C6:E7:F5:04:67:20:BD:C1:74:B3:44:5A:6A:EC:56:36:95:7D:A5:D3:26:69:6D:CE:79:DD:0C:93:6D:1B:A5:4C:6C:D0:10:D8:F2:DC:9E:58:68:07:7A:06:25:74:A0:46:BF:21:34:63:B4:1B:1B:6C:8A:F7:7B:B2:C5:72:B
1:CD:0B:1F:40:D2:7F:8B:A1:35:32:8F:4E:01:EC:0E:ED:CC:03:24:C1:F3:39:54:53:45:22:79:E4:58:98:14:6D:02:F3:FD:56:6D:C2:A9:A6:FC:59:9F:E3:42:F2:9C:C5:79:5E:67:41:AB:CE:6F:D1:D9:9D:0E:B9:5E:B8:DA:55:F2
:6E:00:40:E1:1D:83:34:DA:1B:02:E2:B7:23:16:31:EA:4D:10:A3:75:3D:AC:34:23:53:F8:1D:A9:D2:46:19:25:E4:AE:7A:B0:07:85:56:C7:AE:03:A4:15:24:61:D0:FA:B7:52:BF:C9:C2:14:01:7E:A4:B7:77:AC:8E:D5:90:A4:27:
6B:4C:24:26:F4:84:21:AE:61:D8:20:C6:7A:C5:EB:DF:D5:6F:06:E4:0E:34:36:FF:9C:CF:DA:70:14:23:A4:EB:66:C2:C5:42:8B:C8:51:98:F2:AF:46:FC:DC:AA:95:26:26:55:A1:50:C0:6D:1E:BD:11:73:0E:FE:6C:E3:FD:DA:C
3:40:B4:47:88:40:E7:71:0F:ED:D6:36:E0:2E:7C:66:84:B6:2C:D1:D5:77:59:02:03:01:00:01

Authority Info Access

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*
Issuer Alternative Name	*info@uanataca.com*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.uanataca.com/public/pki/dpc/* *CPS text: [Certificado de la Entidad de Certificación subordinada de UANATACA. Ver http://www.uanataca.com/public/pki/dpc/]*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl* *http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*00:FF:2F:F2:EF:BA:98:C6:B0:23:AD:10:35:55:9A:60:6D:D9:FC:48:A3:9D:34:07:CC:07:A6:78:37:9A:79:09*

X509SubjectName

Subject 2.5.4.97:	*VATES-A66721499*
Subject CN:	*UANATACA CA2 2016*
Subject OU:	*TSP-UANATACA*
Subject O:	*UANATACA S.A.*
Subject L:	*Barcelona (see current address at www.uanataca.com/address)*
Subject C:	*ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-12-16T01:00:00Z

26.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

26.2.3 - History instance n.1 - Status: withdrawn

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by UANATACA CA2 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por UANATACA CA2 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97:	*VATES-A66721499*
Subject CN:	*UANATACA CA2 2016*
Subject OU:	*TSP-UANATACA*
Subject O:	*UANATACA S.A.*
Subject L:	*Barcelona (see current address at www.uanataca.com/address)*
Subject C:	*ES*

X509SKI

X509 SK I	*fVfnYHPOB0ap4qNo8OERsnSSc/0=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*
Status Starting Time	*2018-02-15T01:00:00Z*

26.2.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.2.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by UANATACA CA2 2016*
Name	*[es]*	*Certificados Reconocidos emitidos por UANATACA CA2 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97:	*VATES-A66721499*
Subject CN:	*UANATACA CA2 2016*
Subject OU:	*TSP-UANATACA*
Subject O:	*UANATACA S.A.*
Subject L:	*Barcelona (see current address at www.uanataca.com/address)*
Subject C:	*ES*

X509SKI

X509 SK I	*fVfnYHPOB0ap4qNo8OERsnSSc/0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

26.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.2.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by UANATACA CA2 2016*

Name	[es]	Certificados Reconocidos emitidos por UANATACA CA2 2016

Service digital identities

X509SubjectName

Subject 2.5.4.97:	VATES-A66721499
Subject CN:	UANATACA CA2 2016
Subject OU:	TSP-UANATACA
Subject O:	UANATACA S.A.
Subject L:	Barcelona (see current address at www.uanataca.com/address)
Subject C:	ES

X509SKI

X509 SK I	fVfnYHPOB0ap4qNo8OERsnSSc/0=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision
Status Starting Time	2016-06-14T22:00:00Z

26.3 - Service (granted): Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA – TSU01

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST
Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[en]	Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA – TSU01
Name	[es]	Sellos de tiempo cualificados emitidos por Sello cualificado de tiempo electrónico de UANATACA – TSU01

Service digital identities

Certificate fields details

Version:	3
Serial Number:	1067299580870664226

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIFDCCBfygAwIBAgIIDs/PUGK4ICIwDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBidXlyZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
b59h2GRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEYMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQUSBVEFDQSBDQTIgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzIxNDk5MB4X
DTE3MDUxOTIxMTU1MFoXDTI1MDUxOTIxMTU1MFowgbMxCzAJBgNVBAYTAkVTMRIwEAYDVQQHDAlC
YXJjZWxvbmExFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1VQU5BVEFDQTFH
MEUGA1UEAww+U2VsbG8gY3VhbGlmaWNhZGSgZGUgdGllbXBvIGVzZWN0csOzbmJlbyBkZSBVQU5B
VEFDQSDigJMgVFNVMDExGDAWBgNVBGEMDTZBVETVLUE2NjcyMTQ5OTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMD4wyTu65nG/WUT+5Wb4IyBcOPDcVAtkWPtwyce9YKy+c9Vs6k73EBaf
N583n09+jHnyXN4M6gYOLXlcKhypktMeQHdlyWbHMnxs3gX8EvTbsVGPFLB7MV0HJk0XXoOh3eG
mwwm7+CcILtJp1cc2rybZEsoyuV0+xt05TQz3rOwS5AIq0IZE/1ctPtt4UwyC4pBb+T2fb88IeMx
rSji0ToNKs08nGiEIKasTDiEKsekvEZUDrCqE5VxUvWPA6nPnjvuDswWrr8UDeYGFaUsQCAJd8Uf
vvv5gjmk1AiUsd1NbZeHMciU+FDs+eRBnkKOcmhJAyr+0/iCfpqaH6tBR/8CAwEAAaOCAyMwggMf
MHwGCCsGAQUFBwEDBHAwbjAIBgYEAI5GAQEwCwYGBACORgEDAgEPMAgGBgQAjkYBBDA2BgYEAI5G
AQUwLDAqFiRodHRwczovL3d3dy51YW5hdGFjYS5jb20vcHVibGlj L2Nwcy8TAkVOMBMGBgQAjkYB
BjAJBgcEAI5GAQYCMIHXBggrBgEFBQcBAQSByjCBxzBVBggrBgEFBQcwAoZJaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGlj L2Rvd25sb2FkL3RzcF9jZXJ0aWZpY2F0ZXMvc3Vib3JkaW5hdGUx
LmNydDA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AxLnVhbmF0YWNhLmNvbS9wdW5saWMvcGtpL29j
c3AvMDYyCCSGAQUFBzABhipodHRwOi8vb2NzcDIuaWFuYXRhY2EuY29tL3B1YmxpYy9wa2tvb2Nz
cC8wHQYDVR0OBBYEFO3/1A5NnJeWpqHLJlEPPyigYdtZMAkGA1UdEwQCMAAwHwYDVR0jBBgwFoAU
fVfnYHPOB0ap4qNo8OERsnSSc/0wgaEGA1UdIASBmTCBljCBiAYKKwYBBAGC8TYBBTB6MDAGCCsG
AQUFBwIBFiRodHRwczovL3d3dy51YW5hdGFjYS5jb20vcHVibGlj L2Nwcy8wRgYIKwYBBQUHAgIw
Ogw4Q2VydGlmaWNhZGSgZGUgc2VsbG8gY3VhbGlmaWNhZGSgZGUgdGllbXBvIGVzZWN0csOzbmlj
byduCQYHBACL7EABAzEBjwYDVR0BBiGHMIGEMECgPqABhjpodHRwOi8vY3JsMS1YW5hdGFjYS5j
b20vcHVibGlj L3BraS9jcmwvQ0Eyc3Vib3JkaW5hZGEuY3JsMECgPqAShjpodHRwOi8vY3JsMi51
YW5hdGFjYS5jb20vcHVibGlj L3BraS9jcmwvQ0Eyc3Vib3JkaW5hZGEuY3JsMA4GA1UdDwEB/wQE
AwIHgDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAcBgNVHREEFTATgRFpbmZvQHVhbmF0YWNhLmNv
bTANBgkqhkiG9w0BAQsFAAOCAgEAbNTwLvx2GqRgBMuX+A6rYI+A/VGGVBkJHim0KK/0At1vyew60
2kt1VA72Jlyltqqg0HirM+RFkeu2zwHJd4P+GDj45dSxsc34r7Cul2+gEvDivJcHjYw/qzFHxzxwW
Xq98m4VnoCQtpNnb2RR0BtbCGjYYQR23IJgoxgylo8YCXY+9Xv/z7XsG+FkInIfwGE/nTa/D9bG
L5DlIPjuquPmsw7ldy/14BznZdxjhmhAWCS2Ujz8gLOoEtUvfjylsPAwsu/8zMj1UTlPOHVG0Bj
wiiw7jmCzE5am4ldRIQcwC0IuUJfsGzhBsZrjIVKwC8IsH1WXMQtVSmdb8twPD0kTWtemvOvp1VE
PIPASPlHImirGdLleBbDIceZg4kAmHYPIfpIGrZmhrEO5Awks+LSbsCKIr23uikCpbel8z8TBVjxX
SzUtVjKSzEUctev4D3lH6m+x0avN457YNfhW2WUnGnjb9yAUzGd9bchfH7VUqR0XEVGGNmEfQx27
LuE5foXjo302nmKFAy39+AZ/iefkcgoHGHGg3rD3hRrxNz4dnSjeKA4p4alZAQ/iulhR/qzsP08A
bVjdcvurOk3Q+mWr2Jg5FhIxYDENOv4i20dcf11O4XOtJBV0RHDmnVo4SIvpehg7URXpWful+TCo
CM3g45WggP5ITIB0lBviFq/YmSE=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA2 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *Sello cualificado de tiempo electrónico de UANATACA – TSU01*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona*

Subject C: *ES*

Valid from: *Fri May 19 23:15:50 CEST 2017*

Valid to: *Mon May 19 23:15:50 CEST 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C0:F8:C3:24:EE:EB:99:C6:FD:65:13:FB:95:9B:E0:8C:81:78:E3:C3:79:50:2D:91:63:E2:C3:27:BD:60:AC:BE:73:D5:6
C:EA:4E:F7:10:16:9F:37:9F:37:9F:4F:7E:8C:79:F2:5C:DE:0C:EA:06:0E:2D:72:1C:2A:1C:A9:91:F3:1E:40:77:65:C9:66:C7:32:7C:6C:DE:05:FC:12:F4:DB:B1:51:8F:14:B0:7B:31:5D:07:CC:89:34:5D:7A:0E:87:77:86:9B:0C:
26:EF:E0:9C:24:BA:C8:A5:37:1C:DA:BC:9B:89:91:2C:A3:27:55:D3:EC:74:E5:34:2B:DA:B3:B0:4B:70:1F:AB:47:D9:13:FD:5C:B4:FB:6D:E1:4C:32:0B:8A:41:87:E4:F6:15:BF:3C:21:E3:31:AD:28:E2:D1:3A:0D:2A:CD:3C
:9C:68:84:20:A6:AC:BC:38:84:2A:C7:A4:BC:46:54:0E:B0:AA:13:95:71:52:F5:8F:03:A9:CF:9E:3B:EE:0E:CC:16:AE:BF:14:0D:E6:06:15:A5:2C:40:20:09:77:C5:1F:BE:FB:F9:82:39:A4:D4:08:94:B1:DD:4D:6D:97:87:31:E8:
94:F8:50:EC:F9:E4:41:9E:42:8E:72:68:49:03:2A:FE:D3:F8:82:7E:9A:9A:1F:AB:41:47:FF:02:03:01:00:01

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

id_etsi_qcs_QcSSCD

Authority Info Access	*http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt* *http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*ED:FF:D4:0E:4D:9C:97:96:3E:A1:CB:26:51:0F:3F:28:A0:61:DB:59*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.47286.1.5* *CPS pointer: https://www.uanataca.com/public/cps/* *CPS text: [Certificado de sello cualificado de tiempo electrónico.]* *Policy OID: 0.4.0.194112.1.3*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl* *http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*
Extended Key Usage	*id_kp_timeStamping*
Subject Alternative Name	*info@uanataca.com*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F7:E7:B3:C0:34:02:2E:9F:DD:3E:B2:BD:62:6A:B1:9F:E3:BF:56:D8:DB:20:D6:22:B3:13:17:6D:81:D2:9E:B5*

X509SubjectName

Subject 2.5.4.97:	*VATES-A66721499*
Subject CN:	*Sello cualificado de tiempo electrónico de UANATACA – TSU01*
Subject OU:	*TSP-UANATACA*
Subject O:	*UANATACA S.A.*
Subject L:	*Barcelona*
Subject C:	*ES*

X509SKI

X509 SK I	*7f/UDk2cl5Y+ocsmUQ8/KKBh21k=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*

ETSI 2016 - TSL HR - PDF/A-1b generator

	[es]	*undefined.*
Status Starting Time	*2018-02-15T01:00:00Z*	

27 - TSP: VINTEGRIS S.L.

.

TSP Name

Name	[en]	*VINTEGRIS S.L.*
Name	[es]	*VINTEGRIS S.L.*

TSP Trade Name

Name	[en]	*vinCAsign*
Name	[es]	*vinCAsign*
Name	[en]	*VATES-B62913926*
Name	[en]	*VINTEGRIS SL*
Name	[en]	*Víntegris SL*

PostalAddress

Street Address	[en]	*Avenida Carrillet, 3, Ed. D, 4B*
Locality	[en]	*L´Hospitalet de Llobregat*
State Or Province	[en]	*Barcelona*
Postal Code	[en]	*08092*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*Avenida Carrillet, 3, Ed. D, 4B*
Locality	[es]	*L´Hospitalet de Llobregat*
State Or Province	[es]	*Barcelona*
Postal Code	[es]	*08092*
Country Name	[es]	*ES*

ElectronicAddress

URI	[es]	*mailto:info@vincasign.net*
URI	[es]	*http://www.vincasign.net*

URI	*[en]*	*mailto:info@vincasign.net*
URI	*[en]*	*http://www.vincasign.net*

TSP Information URI

URI	*[en]*	*https://www.vincasign.net/policy/en/*
URI	*[es]*	*https://www.vincasign.net/policy/es/*

27.1 - Service (withdrawn): Qualified Certificates issued by vinCAsign Global Authority

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by vinCAsign Global Authority*
Name	*[es]*	*Certificados Reconocidos emitidos por vinCAsign Global Authority*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *671918045467400215543670222139247462900201383183*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIILzCCBhegAwIBAgIUdbHY4qf9B+WTOts1ZQHMfH2jZQ8wDQYJKoZIhvcNAQELBQAwgcExCzAJ
BgNVBAYMAkVTMRUwEwYDVQQKDAxWSU5URUdSSVMgU0wxTTBLBgNVBAcMREJhcmNlbG9uYSAoc2Vl
IGN1cnJlbnQgYWRkcmVzcyBhdCBodHRwczovL3d3dy52aW5jYXNpZ24ubmV0L2NvbnRhY3QpMRUw
EwYDVQQLDAxFQy1WSU5URUdSSVMxEjAQBgNVBAUTCUI2MjkxNjEhMB8GA1UEAwwYdmluQ0Fz
aWdulFJvb3QgQXV0aG9yaXR5MB4XDTE2MDEyODE0MDIwNloXDTIyMDEyODE0MDIwNlowgcMxCzAJ
BgNVBAYMAkVTMRUwEwYDVQQKDAxWSU5URUdSSVMgU0wxTTBLBgNVBAcMREJhcmNlbG9uYSAoc2Vl
IGN1cnJlbnQgYWRkcmVzcyBhdCBodHRwczovL3d3dy52aW5jYXNpZ24ubmV0L2NvbnRhY3QpMRUw
EwYDVQQLDAxFQy1WSU5URUdSSVMxEjAQBgNVBAUTCUI2MjkxNjEjMCEGA1UEAwwadmluQ0Fz
aWdulEdsb2JhbCBBdXRob3JpdHkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDSmv47
nsYKkz+HX23D0uP0+R7DwzdS9j48oYuQAZvYz10ce6jaAF8ZqCg9HMCPH9m/2D5pyaJIHatN4mnR
IfihFg9FAEmxUPmLjQ4gt0KK2ecayes9uW1mZzeskmjVvoYezlERUdCM52Pl4WHm8ls6rKuYBuL
4lRI5FnCOgyCtuuuMGqNormpYHjw2SlQkJaR1uu0LQYnANK4WV+//NMmyoFcesNOAu+dEvTGMwStn
qHRQXa0hLt/xE31wZzywgLZXDVxXGzPLkW1Qnfxkegb6UjvtcbzYGiz2kzKucWPePsqbYsFornhM
0lVgnOe0cC4IFF36Whvqrgccxiu8lS8M1NqsgwoglkSks4lUQuAJ2WZb8+Uy9muQDDzHN4W31wsYg
z00baXS4jQ7Pndk1w8q4dSJbLI3GgrNVbrwRBTpbHny/tnmvljcG75V4+rQYvTv3z4lJuYwvZDq
A8Fa3cZ06CAC6+oZ29qSc7zGnTPwrdXUTiAZbVOwOLLy+6Bl0bGUu8cdcc761Z84kVZycFW/kF+yp
v1s8jlYBlvVLPBTk/Ex5PGBMLklHDvJnyyw6EkbACYJrho6UkE2cUB+heUKxMFzHLToylQWzTzb
sdLQvl8gPOcGXcHbUMLmYAZYcQOHPiGakLoiApIVxuO5Qk+bxkdC04xWa2lBcCLFhapwgwIDAQAB
o4ICGTCCAhUwHwYDVR0jBBgwFoAUqYqtWt6OGAt0izDtJ5kTgMQMwHQYDVR0OBBYEFAdGy0vl
15hc0R6BCCv4bqMNN7LMA4GA1UdDwEB/wQEAwIBBjCBzAYDVR0gBIHEMIHBMIG+BgRVHSAAMIG1
MCgGCCsGAQUFBwIBFhxodHRwczovL3BvbGlyeS52aW5jYXNpZ24ubmV0MIGlBggrBgEFBQcCAjB8
DHpDZXJ0aWZpY2FkbyBkZSBsYSB2aWSDQXNpZ24gR2xvYmFsIEF1dGhvcml0eSBkZSBsYSBFbnRp
ZGFkIGRlIGNlcnRpZmlj YWNpb24gZGUgVmludGVncmlzLiBWZXIgaHR0cHM6Ly9wb2xpY3kudmlu
Y2FzaWdtul.m5ldDAdBgNVHBEEFjAUgRJpbnZcQHZpbmNlc2lnbi5uZXQwYQYDVR0fBFowWDAqoCig
Jo YkaHR0cDovL2NvbDEudmluY2FzaWdulm5ldC9jYXJvb3QuY3sMCgqKAmhiKodHRwOh8vY3Js
Mi52aW5jYXNpZ24ubmV0L2Nhcm9vdC5jcmwwXgYIKwYBBQUHAQEEUjBQMCYGCCsGAQUFBzABhhpo
dHRwOi8vb2NzcDEudmluY2FzaWdulm5ldDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3AyLnZpbmNh
c2lnbi5uZXQwEgYDVR0TAQH/BAgwBgEB/wIBATANBgkqhkiG9w0BAQsFAAOCAgEARtIaIiZHC0SO
GvL5cdWzS5UAoj1z/dOwrlZ7CDpI4v4qEPsBIFo5XQdcvC0ex/47WqkS0SwISHRH6KPbJzroBe
a//PrmKTzphnLiTJ91jhF20lXR52NSgXVglRK3+R1Pmwas5M9917cBN1ZLUlFB/ZA/3uabl9nawg
liOzN5GFpomxNmWZVBrrGxKXLz7JmC6nRrcuOAT5a0QaDYtvwQv2YAd6FR/U8gkXaW7T6lVNdJ5x
uLlwlgavuLNycmh4/6smuvMhXoscoG9KArcIdduCkLkTY/BHPb4P7ruohdrBEKRskTIoiQkR/7j
GTqKIzvsx/1vPNuKA5hP5YvRT2w6sXknF+JRmUjboUnzLtQT9gsIe7M4VnqVMt+O7hGP7oKboz
1PPCnVVGhXW4I7oSWd8ecJZI6vgYd5IZuiSOk3keCChTJOQOl0t279KChbE5mcccO7lH3ST2VTGW
aFXVa4IleCiwOYDjGKd04O/TWc2nftWEd72UEfL5XRDRSL+GOcm9T5dc3GoWOMs1uaPjcANxR1eR
6JYP65pLbOnmXNB5l0xOANkCYx1k52bjsZh74mnU/KxJferfY+gBqBO4bJ0xsbTvWpbr/v9c79WU
nJMY4Zik8eb0+OdsxcT8PH6owBKR4On0BPEN23zbOAv8vnHbbfOMZ8IbIHhMiY=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *vinCAsign Root Authority*

Issuer SERIAL NUMBER: *B62913926*

Issuer OU:	*EC-VINTEGRIS*
Issuer L:	*Barcelona (see current address at https://www.vincasign.net/contact)*
Issuer O:	*VINTEGRIS SL*
Issuer C:	*ES*
Subject CN:	*vinCAsign Global Authority*
Subject SERIAL NUMBER:	*B62913926*
Subject OU:	*EC-VINTEGRIS*
Subject L:	*Barcelona (see current address at https://www.vincasign.net/contact)*
Subject O:	*VINTEGRIS SL*
Subject C:	*ES*
Valid from:	*Thu Jan 28 15:02:06 CET 2016*
Valid to:	*Fri Jan 28 15:02:06 CET 2022*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:9A:FE:3B:9E:C6:0A:93:3F:87:5F:6D:C3:D1:A3:F4:F9:1E:C3:C3:37:52:F6:3E:3C:A1:8B:90:01:9B:D8:CF:5D:1C:7B:A8:DA:00:5F:19:A8:28:3D:1C:C0:8F:1F:D9:BF:D8:3E:69:C9:A2:48:1D:AB:4D:E2:69:D1:21:F8:A1:16:0F:45:00:49:B1:50:F9:8B:8D:0E:20:D0:A2:B6:79:C6:B2:7A:CF:6E:FD:6D:66:67:37:AC:92:68:E5:56:FA:18:7B:42:04:45:47:42:33:9D:8F:97:85:87:9B:C8:79:AF:A2:AE:60:1B:8B:E2:54:48:E4:59:C2:3A:0C:82:BA:EB:8C:1A:A3:68:AE:6A:58:1E:3C:36:4A:54:24:25:A4:75:BA:E3:8B:41:89:C0:34:AE:16:57:EF:FF:34:C9:B2:A0:57:1E:68:D3:80:BB:E7:44:BD:31:8C:C1:2B:67:A8:74:50:5D:AD:21:2E:DF:F1:13:7D:70:67:3C:B0:80:B6:57:0D:5C:57:1B:33:CB:91:6D:50:9D:FC:64:7A:00:5C:52:3B:ED:71:BC:D8:1A:2C:F6:93:32:AE:71:63:DE:3E:CA:9B:62:C1:68:AE:78:4C:D1:F5:60:9C:E7:B4:70:2E:1F:14:5D:FA:5A:1B:EA:AE:07:1C:C6:2B:BC:95:2F:0C:D4:DA:AC:83:0A:20:96:44:A4:B3:85:10:B8:02:76:59:96:FC:F9:4C:BD:9A:E4:03:0F:31:CD:E1:6D:F5:C2:C6:20:CF:4D:1B:69:74:B8:8D:0E:CF:9D:D9:13:C3:CA:B8:75:22:5B:2C:8D:C6:82:B3:55:6E:B2:70:44:14:E9:6C:79:F2:FE:D9:E6:BE:58:DC:1B:BE:55:E3:EA:D0:62:F4:EF:DF:3E:1F:26:E6:30:BD:90:EA:03:C1:5A:DD:C6:4E:E8:20:3A:FA:86:76:F6:A4:9C:EF:31:A7:4C:FC:2B:75:74:D4:20:06:5B:54:EC:0E:2C:BC:BE:E8:12:34:84:65:2E:05:C9:1E:EF:AD:59:F3:89:15:67:27:05:5B:F2:64:17:EC:A9:BF:5B:3C:8E:58:D8:04:8B:D5:2C:F0:53:93:F1:31:E4:F1:81:30:B9:08:1C:3B:C9:9F:2C:B0:E8:49:1B:00:26:09:AE:1A:3A:52:41:36:71:40:7E:85:E5:0A:C4:C1:73:1C:B4:CE:CA:54:16:CD:3C:DB:B1:D2:D0:BC:8F:20:3C:E7:06:5D:C1:E1:50:C2:E6:60:06:58:79:03:87:3E:21:9A:90:BA:22:02:97:D5:C6:E3:B9:42:4F:9B:C6:47:42:D3:8C:56:6B:69:41:70:22:C5:85:AA:70:83:02:03:01:00:01*
Authority Key Identifier	*A9:8A:AD:59:FD:ED:E8:E1:80:8B:48:B3:0E:D2:63:E6:44:E0:31:03*
Subject Key Identifier	*07:46:CB:4B:E5:D4:8E:61:73:44:7A:04:20:B2:E1:BA:8C:34:DE:CB*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.vincasign.net* *CPS text: [Certificado de la vinCAsign Global Authority de la Entidad de certificacion de Vintegris. Ver https://policy.vincasign.net]*
Subject Alternative Name	*info@vincasign.net*
CRL Distribution Points	*http://crl1.vincasign.net/caroot.crl* *http://crl2.vincasign.net/caroot.crl*
Authority Info Access	*http://ocsp1.vincasign.net* *http://ocsp2.vincasign.net*
Basic Constraints	*IsCA: true - Path length: 1*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *30:5E:88:A5:EB:B7:DA:E9:E6:6B:F8:A3:D2:1E:64:3C:C2:09:5C:18:FF:7A:F4:7D:FE:1B:AB:2B:88:1D:CB:F8*

X509SubjectName

Subject CN: *vinCAsign Global Authority*

Subject SERIAL NUMBER: *B62913926*

Subject OU: *EC-VINTEGRIS*

Subject L: *Barcelona (see current address at https://www.vincasign.net/contact)*

Subject O: *VINTEGRIS SL*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2017-12-20T01:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

27.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.5.2*

27.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.1.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by vinCAsign Global Authority

Name [es] Certificados Reconocidos emitidos por vinCAsign Global Authority

Service digital identities

X509SubjectName

Subject CN: vinCAsign Global Authority

Subject SERIAL NUMBER: B62913926

Subject OU: EC-VINTEGRIS

Subject L: Barcelona (see current address at https://www.vincasign.net/contact)

Subject O: VINTEGRIS SL

Subject C: ES

X509SKI

X509 SK I B0bLS+XUjmFzRHoEILLhuow03ss=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

27.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.5.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.5.2

27.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by vinCAsign Global Authority

Name [es] Certificados Reconocidos emitidos por vinCAsign Global Authority

Service digital identities

X509SubjectName

Subject CN: vinCAsign Global Authority

Subject SERIAL NUMBER: B62913926

Subject OU: EC-VINTEGRIS

Subject L: Barcelona (see current address at https://www.vincasign.net/contact)

Subject O: VINTEGRIS SL

Subject C: ES

X509SKI

X509 SK I B0bLS+XUjmFzRHoEILLhuow03ss=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2016-06-21T22:00:00Z

27.1.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.5.2*

27.2 - Service (withdrawn): Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en]	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority*
Name	*[en]*	*Qualified Certificates issued by vinCAsign nebulaSUITE Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *580247578624264002174382824980712041798116291597*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH6jCCBdKgAwIBAgIUZaMzriOC5tApthPDHOq+c//XDtA0wDQYJKoZIhvcNAQELBQAwgZ0xCzAJ
BgNVBAYTAkVTMRYwFAYDVQQKDAJ1Ww61udGVncmlzIFNMMSAwHgYDVQQHDBdIb3NwaXRhbGV0IGRl
IExsb2JyZWdhdDEYMBYGA1UEYQwPVkFURVMtQjYyOTEzOT12MSYwJAYDVQQDDB12aW5DQXNpZ24g
UXVhbGlmaWVkIEF1dGhvcml0eTESMBAGA1UECAwJQmFyY2Vsb25hMB4XDTE3MDQyMDEwMTkzNVoX
DTMwMDQyMDEwMTkzNVowgZ8xCzAJBgNVBAYTAkVTMRYwFAYDVQQKDA1Ww61udGVncmlzIFNMMSAw
HgYDVQQHDBdIb3NwaXRhbGV0IGRlIExsb2JyZWdhdDEYMBYGA1UEYQwPVkFURVMtQjYyOTEzOTI2
MSgwJgYDVQQDDB92aW5DQXNpZ24gbmVidWxhU1VJVEUgQXV0aG9yaXR5MRIwEAYDVQQIDAlCYXJj
ZWxvbmEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDGHrxpkfe7yWAw0+q60bFetfpJ
0gaD9cMaDTfcJq+uZvQOFrKKXgYXqdjkq5DkJkN87MrJlKIkyKrHSbdKJJmC7++evpO6GBWIIw
7RIkIEPzrVacBUIG2Z60kcXYZC6S09IPbAHRwWHDf4mMMLCiY9lcZA79kqnPk5MW1NRx1oEgpg5k
XFRhnCWW8FBCNv8pcLjujpd7MdnuGrOsZ56Mz/BANCii0Ob312UVvxhmxB4GCHPfEWt7K3ht8GY
RSGpKS3EzPq/i8dlokdvyt2fgDUzYfM0Yo6CqWER2I4AUfBGh36YEQ1NLiKj3Jzr4JnOSGkjiCLZ
oIY9gkEEfxFmpFMBmK1uycQzo0ECJP7mJ8STixJpty/a7sFMR2/QJqYK2UG6LIqFW6k2plgkhroT
oPsQl0OE+uxT5g5YzI2Ij2A00X/VXXPiZIxpV1jlCyDzGIJvIyrIoZISIm1Z2S9oIlsV1YxcVK0
j1IsokyaVCH0qv/VSzcf0kcHW31cDFfH8AU2TVpYmwKWr4L/b36xx6OIvOhxIc3YSYSv64rAK2MonN
4mwlj/nI7jt+p0Zrnz+NiSWhjt1MtI8AdGv95IVMzhXdz+Np0oiUnf5UGIG2hLoL7cWvPHtAJWCk
AJj8U/sk3UaXHuqcphYfjM4NXYNGYxyyfEb3aL WHwa/6bZyGCiwDAQABo4ICHDCCAhgwHwYDVR0j
BBgwFoAU0D5KapJvTbOGR1xt05FgAvQWyNAwHQYDVR0OBBYEFIRr76lnnaYKzR96e98XXnwY1KSk
MA4GA1UdDwEB/wQEAwIBBjCBjAYDVR0gBIGEMIGBMH8GBFUdIAAwdzAoBggrBgEFBQcCARYcaHR0
cHM6Ly9wb2xpY3kudmluY2FzaWduLm5ldDBLBggrBgEFBQcCAjA/DD1DZXJ0aWZpY2FkbyBDQSBT
dWJvcmRpbmFkYS4gVmVyICBodHRwczovL3BvbGljeS52aW5jYXNpZ24ubmV0MB0GA1UdEQQWMBSB
EmluZm9AdmluY2FzaWduLm5ldDBIBgNVH R8EWDBWMCmgJ6AlhNodHRwOi8vY3JsMy52aW5jYXNp
Z24ubmV0L2Nhc3VzLmNybDApoCcgJYYjaHR0cDovL2NybDQudmluY2FzaWduLm5ldC9YXNlYy5j
cmwwgaIGCCsGAQUFBwEBBIGVMIGSMCYGCCsGAQUFBzABhhpodHRwOi8vb2NzcDMudmluY2FzaWdu
Lm5ldDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3A0LnZpbmNhc2lnbi5uZXQwQAYIKwYBBQUHMAKG
NGh0dHBzOi8vd3d3LnZpbmNhc2lnbi5uZXQvcHVibGlja2V5cy9jYXF1YWxpZmllZC5jZXJwEgYD
VR0TAQH/BAgwBgEB/wIBATANBgkqhkiG9w0BAQsFAAOCAgEAQZ6CjTzGguTSTJpXDKYWJfjBRtQ
cDN4/WIZW9Ze2wPabYA5GlkN056xLuHaKnnhcmjtOz96CbWgPzMDxEKHNqDF7Izkko+/0kZOuBwE
p4Sn2xPsWF8/cyxqZ4srpN8C/gK2NZN+qOVrJa3Pvtahq7mzDgOA/mzuk5xoEDAD0iHLdnXrjPJU
Hr54NUskmhu/pOX3MwBiIj2sDYBOVAWBIDeMPRICbGIAsZx1ZqOSUWp1WaamzsA81pMfxcelJ61NO
WRQ0BtrtOYg2OuUHVVLBm3/YEgVkPHq3kNKdFo6N0Csbf VToEuSk7TIkadBQ062q+JOs59gQbd/
QWwfjzIliSaHLzY4uVaazJiMi0daKD76QvPXxDrG3Ym0yghuPGU2D+kmkalrumbhkml6+8C2qgX
C+wlbQLUnUg4LC5IQWKIKHzRdRaeZaExrp6MteIdHjmsBTG/O3bAVYIcS+0kW863tygAPlFQxBeh
UvcDaJD6yJwcZn7vTbOmJUR62GVKfoPU/+alChlZwXb6YRNX7cDC73N5DAA4MMFsIT s2F/HczjohQ
2KcMgn9QfYoldrH8+GeCMyUu3pb3vnXLUvJhNaLZQOsQvSmyQvNoT+LM9qdVnM4l/Mn0WyQi
Q59a+8aTlLYHF57G7XUyjcMF12U7YPNa/oOpCTOSp73VTdE=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer ST:	*Barcelona*
Issuer CN:	*vinCAsign Qualified Authority*
Issuer 2.5.4.97:	*VATES-B62913926*
Issuer L:	*Hospitalet de Llobregat*
Issuer O:	*Víntegris SL*
Issuer C:	*ES*
Subject ST:	*Barcelona*
Subject CN:	*vinCAsign nebulaSUITE Authority*
Subject 2.5.4.97:	*VATES-B62913926*
Subject L:	*Hospitalet de Llobregat*
Subject O:	*Víntegris SL*
Subject C:	*ES*
Valid from:	*Thu Apr 20 12:19:35 CEST 2017*
Valid to:	*Sat Apr 20 12:19:35 CEST 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C6:1E:BC:69:91:F7:BB:C9:60:30:D3:EA:BA:D1:B1:5E:B5:FA:49:D2:06:83:F5:C3:1A:0D:37:09:72:3F:AE:DB:34:10:7C:5A:CA:29:78:18:5E:A7:63:92:AE:43:90:99:0D:F3:B3:2B:25:B2:0A:B6:4C:8A:AC:74:9B:74:A2:49:98:2E:FE:F9:EB:E9:3B:A1:81:59:FB:70:ED:12:24:20:43:F3:AD:F5:5A:70:15:08:19:9F:34:92:25:D8:D8:2E:92:97:D9:4F:84:01:D1:C1:61:C3:23:89:8C:30:B0:A2:63:D2:1C:64:0E:FD:96:AB:8F:93:93:16:D4:D4:6F:26:81:20:A6:0E:64:5C:54:61:9C:25:96:F0:50:42:36:FF:29:70:B8:EE:8E:97:7B:31:D9:EE:1A:B3:AC:67:9E:8C:CF:F0:40:34:28:A2:D0:E6:F7:D7:65:15:BF:18:5A:9F:10:78:18:21:CF:7C:45:9F:EC:AD:E1:B7:C1:98:45:21:A9:29:2D:C4:CC:FA:BF:8B:C7:65:A2:47:6F:CA:DD:9F:80:35:33:61:F3:34:62:8E:82:A9:61:11:D8:8E:00:51:FB:41:1A:1D:FA:60:44:35:34:B8:8A:8F:72:73:E0:99:CE:48:69:23:88:22:D9:A0:86:3D:82:41:04:7E:11:66:A4:53:01:98:AD:6E:C9:C4:33:A3:41:02:24:FE:E6:27:C4:93:8B:12:69:B7:2F:DA:EE:C1:4C:47:6F:D0:26:A6:0A:D9:41:BA:2C:8A:85:5B:A9:36:A4:88:24:86:BA:13:A0:FC:D0:7F:43:84:FA:EC:53:E6:0E:58:AE:5D:88:8F:60:34:D1:72:7F:55:75:CF:DD:99:76:C6:95:75:8C:80:B2:0F:31:88:26:F2:32:AE:5A:19:21:22:26:4F:66:7D:A0:89:6C:57:56:31:71:52:B4:8E:22:2C:A2:4C:9A:54:21:F4:AA:FF:D5:49:97:19:D2:47:87:5B:7D:5C:0C:57:C7:F0:05:36:4D:5A:58:9B:02:96:AF:85:1B:DF:AC:7A:38:8B:CE:87:FC:48:71:84:98:F2:FE:B8:AC:02:B6:32:89:CD:E2:6C:25:8F:F9:C8:EE:3B:7E:A7:46:6B:9F:3F:8D:89:25:A1:8E:DD:4C:B4:8F:00:74:6B:FD:E6:55:4C:CE:15:DD:CF:E3:69:D2:88:94:9D:FE:54:19:F1:B6:84:BA:0B:ED:C5:AF:3C:7B:40:25:60:A4:00:98:FC:52:C9:37:51:A5:C7:BA:A7:29:85:87:E3:33:83:57:60:D1:98:C7:2C:9F:11:BD:DA:2D:61:F0:6B:FE:9B:67:21:82:7F:02:03:01:00:01*
Authority Key Identifier	*D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0*
Subject Key Identifier	*84:6B:EF:A2:27:9D:A6:0A:AD:1F:7A:AF:DF:17:5E:7C:18:D4:A4:A4*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.vincasign.net* *CPS text: [Certificado CA Subordinada. Ver https://policy.vincasign.net]*
Subject Alternative Name	*info@vincasign.net*
CRL Distribution Points	*http://crl3.vincasign.net/casub.crl* *http://crl4.vincasign.net/casub.crl*
Authority Info Access	*http://ocsp3.vincasign.net* *http://ocsp4.vincasign.net* *https://www.vincasign.net/publickeys/caqualified.cer*

Basic Constraints *IsCA: true - Path length: 1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D7:CD:55:49:04:DF:D2:2A:22:EB:96:5C:E0:1B:B1:A3:0C:21:51:CA:07:47:3D:4C:BD:45:DF:5D:AF:27:36:A4*

X509SubjectName

Subject ST: *Barcelona*

Subject CN: *vinCAsign nebulaSUITE Authority*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *Hospitalet de Llobregat*

Subject O: *Víntegris SL*

Subject C: *ES*

X509SKI

X509 SK I *hGvvoiedpgqtH3qv3xdefBjUpKQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-10-08T01:00:00Z*

27.2.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.6.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.11*

Description

27.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.2.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority*
Name	*[en]*	*Qualified Certificates issued by vinCAsign nebulaSUITE Authority*

Service digital identities

X509SubjectName

Subject ST:	*Barcelona*
Subject CN:	*vinCAsign nebulaSUITE Authority*
Subject 2.5.4.97:	*VATES-B62913926*
Subject L:	*Hospitalet de Llobregat*
Subject O:	*Víntegris SL*
Subject C:	*ES*

X509SKI

X509 SK I	*hGvvoiedpgqtH3qv3xdefBjUpKQ=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2017-12-20T01:00:00Z*

27.2.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.6.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.11*

Description

27.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.3 - Service (granted): Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority*

Name *[en]* *Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *637401987826912361881659849906312446373074387053*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHjCCBeagAwIBAgIUb6YX+bvL5BQJcCgnTDqWu/n9QG0wDQYJKoZIhvcNAQELBQAwgZ0xCzAJ
BgNVBAYTAkVTMRYwFAYDVQQKDA1Vbw61udGVncmlzIFNMMSAwHgYDVQQHDBdlb3NwaXRhbGV0IGR1
IExsb2lyZWdlaDEYMBYGA1UEYQwPVAFURVMtQyYvOTEzOTZMSYwJAYDVQQDDB12aW5DQXNpZ24g
UXVhbGlmaWVkIEF1dGhvcml0eTESMBAGA1UECAwJQmFyY2Vsb25hbMB4XDTE3MDkyNzE0MjA0NloX
DTMwMDkyNzE0MjA0NlowgbMxCzAJBgNVBAYTAkVTMRIwEAYDVQQIDAlCQVJDRUxPTkExIDAeBgNV
BAcMF0hPU1BJVEFMRVQgREUgTExPQUFR0FUMRgwFgYDVQRhDA9WQVRFUy1CNjI5MTM5MjYxEjAQ
BgNVBAsMCXZpbkNBc2lnbjEVMBMGA1UECgwMVkIOVEVIUkITIFNMMSkwJwYDVQQDDCB2aW5DQXNp
Z24gbmVidWxhU1VJVEUyIEF1dGhvcml0eTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
AM/OdTCod0+jr2EHGWuR1480Vx0GHoR0PUoORtzoqRHp51r00rtSO0925w8pHlzuyQS7WhZnpWwL
IY2CcJGSO6bIZ57ZaGiHyHEKRPnUVWZL5v6QNqHfgD7/Vl7Ldoj3aY5Lg71Wpx8G+NmBsYHwz8a2
yAtD0RDVbxZrmZD5pfvPsTq3tb2zBq1UnYmuaYyNkw8z1s3NpyHN98BXCQYTsLbXP75guLAX2lHt
jLeFny0KPn0PPjpXvoO0w7O+JYxdMU/Fmu03qIeQb23tf/dQB4bTba2sXixGeVgc78RWFdjsHIY
FrLvrw3ISjicqbooJDOPRyG7LTSLk7mv6tZiOTYZT155WYDUV0WbJAp+5GZmOszMpZ5tW5nEi7+O
Ed0xT1i0CPB9mzyr4EfypPBTg2yairUGN2iQ+azSKYybUj/B/S+qADB/ypDi5bT/NG16S5RwuWd1
oxNsnon2gq3cPIlDTI1TJxgYolRGJyU4cgNXUbV/DTGsm43FXY67JYuuOvCgPlKmyGfs1Rtq4+Km
61cfCzmIVAKXsr6Dp9fbNLAIpVhbk1VsKb7tYhrME1WmCsor9e1u66qcWKeXOw2Fzf4TqsEgRL
BHdha1w0ugF33hTGy+w9FuZL+QVGT5nsDlt5exJvzapRfAfHN+Lqv59TWj4neNydsAfAgngN9NfB
AgMBAAGjggIcMIICGDAfBgNVHSMEGDAWgBTQPkpqkm9Ns4ZHXHTkVqMC9Bhl0DAdBgNVHQ4EFgQU
TdZ6hiuc9kt699v96VFML3fcFn4wDgYDVR0PAQH/BAQDAgEGMIGMBgNVHSAEgYQwgYEwfwYEVR0g
ADB3MCgGCCsGAQUFBwIBFhxodHRwczovL3BvbGlzeS5zaW5jYXNpZ24ubmV0MEsGCCsGAQUFBwIC
MD8MPUNlcnRpZmlyYWRvIENBIFN1Ym9yZGluYWRhLiBWZXIgIGh0dHBzOi8vcG9saWN5LnZpbmNh
c2lnbi5uZXQwHQYDVR0RBBYwFIESaW5mb0B2aW5jYXNpZ24ubmV0MF8GA1UdHwRYMFYwKaAnoCWG
I2h0dHA6Ly9jcmwzLnZpbmNhc2lnbi5uZXQvY2FzdWluY3J8MCmgJ6AhiNodHRwOi8vY3JsNC52
aW5jYXNpZ24ubmV0L2Nhc3YuLmNybDCBogYIKwYBBQUHAQEEgZUwgZIwJgYIKwYBBQUHMAGGGmh0
dHA6Ly9vY3NwMy52aW5jYXNpZ24ubmV0MCYGCCsGAQUFBzABhhpodHRwOi8vb2NzcDQudmluY2Fz
aWduLm5ldDBABggrBgEFBQcwAoY0aHR0cHM6Ly93d3cudmluY2FzaWduLm5ldC9wdWJsaWNrZXlz
L2NhcXVhbGlmaWVkLmNlcyASBgNVHRMBAf8ECDAGAQH/AgEBMA0GCSqGSIb3DQEBCwUAA4ICAQDQ
xhZRSjIodlLHgoPKv75J18Tx7Ks6DLHBjTPTuGbzYdZVkJVjQC1CPYvCQmaInq5OCgc2XS1M9JMG6
PgCdzo//roQXE/YJJ9wwhvNKKaMz5WcCdHpJlFiPipZT8EZcWH4NFy5AIN929AEEZ6Fsu20JzQt
GsUeufguuXGcFw19J3T5ikQCCl2EjD1rv3mpDLNs/K9GB9mmbkG90Y8qj4ERICQLIMbWCkKLDT91
0tX9d7+vnxyRpua3geQQECdpd1yr1jSGjBSchyxId9hh7ptGPIqUI0dIXlbxkEXgZ6vo/3SIBfdt
Bg8Obug3vL5w/JnZ+4+uJXSpI/QCqMCWKeJerigxvzMROT1cl0HvZaVnNYpYyhL6nr7X89/K5N
t4R6uBtklH6iUAhYaoeTTMSgGyMUkT+YDSbNPlZXOEuz+FC7SVQIf0/cr10gJxqLHWXbnC44mw
FbfUskxvLukRB47kZEC8NLLAQxskK7mfb+ACx2Ec7815n9FixZ/2xWUGV+0iEciReqaHiWqTcNe
r/VLdpaeSpizqKdQbi+DzxOGyFQxHhH3mBfnNZ3JEd4EOtZ6m/GbD4V6Iq1PYbWCjCqtynWYr34
DInE09q+Y7oC/ynuQJx4lGJtQjDjJ4pxuyXQW9FC5GCTz7t1FHeydLA/cqMPFV0WhdvUgOVGjA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer ST: *Barcelona*

Issuer CN: *vinCAsign Qualified Authority*

Issuer 2.5.4.97: *VATES-B62913926*

Issuer L: *Hospitalet de Llobregat*

Issuer O: *Víntegris SL*

Issuer C: *ES*

Subject CN: *vinCAsign nebulaSUITE2 Authority*

Subject O:	*VINTEGRIS SL*
Subject OU:	*vinCAsign*
Subject 2.5.4.97:	*VATES-B62913926*
Subject L:	*HOSPITALET DE LLOBREGAT*
Subject ST:	*BARCELONA*
Subject C:	*ES*
Valid from:	*Wed Sep 27 16:20:46 CEST 2017*
Valid to:	*Fri Sep 27 16:20:46 CEST 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CF:CE:75:30:A8:77:4F:A3:AF:61:07:19:6B:91:D7:8F:34:57:1D:06:1E:84:74:3D:4A:0E:46:BC:E8:A9:11:E9:E7:5A:F4:D2:BB:52:3B:4F:76:E7:0F:29:1E:5C:EE:C9:04:BB:5A:16:67:A5:6C:0B:95:8D:82:70:91:92:3B:A8:48:67:9E:D9:68:68:87:C8:71:0A:44:F9:D4:55:66:4B:E6:FE:90:36:A1:DF:80:3E:FF:56:5E:CB:76:88:F7:69:8E:4B:83:BD:56:A7:1F:06:F8:D9:81:B1:81:F0:CF:C6:B6:C8:0B:43:D1:10:D5:87:16:6B:99:90:F9:A5:FB:CF:B1:3A:B7:B6:1D:B3:06:AD:54:9D:89:AE:69:8C:8D:93:0F:2B:2E:CD:CD:A7:21:CD:F5:20:57:09:06:13:B0:B6:D7:3F:BE:60:68:B0:17:DA:51:ED:8C:B7:9A:16:7C:B4:28:F9:F4:3C:F8:E9:5E:FA:0E:D3:0E:CE:F8:96:31:74:C5:05:9A:ED:37:A8:87:90:87:6D:ED:7F:F7:7F:40:1E:1B:4D:B6:B6:B1:78:B1:19:E5:60:73:BF:11:58:57:63:B0:72:58:16:B2:EF:AF:0D:C8:4A:38:9C:A9:BA:28:24:33:8F:47:21:BB:2D:34:8B:93:B9:AF:EA:D6:62:39:36:19:4F:5E:79:59:80:D4:57:45:9B:24:0A:7E:E4:66:66:3A:CC:CC:A5:9E:6D:5B:99:C4:8B:BF:8E:11:DD:31:4F:58:B4:08:F0:7D:9B:3C:AB:E0:47:EF:A4:F0:53:83:6C:9A:8A:B5:06:37:68:90:F9:AC:D2:29:8C:9B:52:3F:C1:FD:2F:AA:00:30:7F:CA:90:E2:E5:B4:FF:34:6D:7A:4B:94:70:B9:67:75:A3:13:6C:9E:89:F6:82:AD:DC:3C:82:03:4C:8D:53:27:18:18:A0:84:46:27:25:38:72:03:57:51:B5:7F:0D:31:AC:9B:8D:C5:5D:8E:BB:8D:8B:AE:3A:F0:A0:3E:52:A6:C8:67:EC:D5:1A:EA:E3:E2:A6:EB:57:2D:09:C9:A5:54:02:97:B2:BE:83:A7:D7:DB:34:B0:25:8A:95:61:6E:42:15:B0:A8:7B:8D:88:6B:30:4D:56:98:2B:28:AF:D7:B5:BB:AE:AD:81:E5:8A:79:73:B0:D8:5C:E5:E1:3A:AC:12:04:4B:04:77:61:6B:5C:34:6A:01:77:DE:14:C6:CB:EC:3D:16:E6:4B:F9:05:46:4F:99:EC:0E:5B:79:7B:12:6F:CD:AA:51:7C:07:C7:37:E2:EA:BF:9F:5F:5A:3E:27:78:DC:9D:B0:07:C0:82:98:0D:F4:D7:C1:02:03:01:00:01*
Authority Key Identifier	*D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0*
Subject Key Identifier	*4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.vincasign.net* *CPS text: [Certificado CA Subordinada. Ver https://policy.vincasign.net]*
Subject Alternative Name	*info@vincasign.net*
CRL Distribution Points	*http://crl3.vincasign.net/casub.crl* *http://crl4.vincasign.net/casub.crl*
Authority Info Access	*http://ocsp3.vincasign.net* *http://ocsp4.vincasign.net* *https://www.vincasign.net/publickeys/caqualified.cer*
Basic Constraints	*IsCA: true - Path length: 1*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*DA:13:26:D2:2E:64:F7:C2:1F:38:81:21:F6:8C:8F:70:0D:30:5C:69:FB:0B:5E:8B:9F:C2:84:6F:7A:E7:CB:70*

X509SubjectName

Subject CN:	*vinCAsign nebulaSUITE2 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *TdZ6hiuc9kt699v96VFML3fcFn4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2019-11-06T01:00:00Z

27.3.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.1.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.6.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.4.1*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.2.11

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.1.51

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.2.51

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.2.151

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.4.11

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.6.51

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.10.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.10.51

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.11.1

Description

27.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

27.3.4 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority

Name [en] Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority

Service digital identities

X509SubjectName

Subject CN: vinCAsign nebulaSUITE2 Authority

Subject O: VINTEGRIS SL

Subject OU: vinCAsign

Subject 2.5.4.97: VATES-B62913926

Subject L: HOSPITALET DE LLOBREGAT

Subject ST: BARCELONA

Subject C: ES

X509SKI

X509 SK I TdZ6hiuc9kt699v96VFML3fcFn4=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2019-10-28T01:00:00Z

27.3.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.1.1

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.6.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.4.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.2.11*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.1.51*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.2.51*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.2.151*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.4.11*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.6.51*

Description

27.3.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.3.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.3.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority*
Name	*[en]*	*Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority*

Service digital identities

X509SubjectName

Subject CN:	*vinCAsign nebulaSUITE2 Authority*
Subject O:	*VINTEGRIS SL*
Subject OU:	*vinCAsign*
Subject 2.5.4.97:	*VATES-B62913926*
Subject L:	*HOSPITALET DE LLOBREGAT*
Subject ST:	*BARCELONA*
Subject C:	*ES*

X509SKI

X509 SK I	*TdZ6hiuc9kt699v96VFML3fcFn4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-08-02T00:00:00Z*

27.3.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.6.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.4.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.11*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.1.51*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.51*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.151*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.4.11*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.6.51*

Description

27.3.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.3.5.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

27.3.6 - History instance n.3 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority

Name [en] Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority

Service digital identities

X509SubjectName

Subject CN: vinCAsign nebulaSUITE2 Authority

Subject O: VINTEGRIS SL

Subject OU: vinCAsign

Subject 2.5.4.97: VATES-B62913926

Subject L: HOSPITALET DE LLOBREGAT

Subject ST: BARCELONA

Subject C: ES

X509SKI

X509 SK I TdZ6hiuc9kt699v96VFML3fcFn4=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2018-04-09T00:00:00Z

27.3.6.7 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.1.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.6.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.4.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47155.1.2.11*

Description

27.3.6.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.3.6.9 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.4 - Service (granted): Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE1 Authority

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[es]*	*Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE1 Authority*
Name	*[en]*	*Qualified time stamps issued by vinTSAsign nebulaSUITE1 Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6235309547980698782*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJSzCCBzOgAwIBAgIIVohE/2/9tJ4wDQYJKoZIhvcNAQENBQAwgbMxCzAJBgNVBAYTAkVTMRIw
EAYDVQQDDAlCQVJDRUxPTkExIDAeBgNVBAcMF0hPU1BJVEFMRVQgREUgTExPQUFR0FUMBgwFgYD
VQRbDA9WQVRFUy1CNjI5MTM5MjYxEjAQBgNVBAsMCXZpbkNBc2lnbjEVMBMGA1UECgwMVklOVEVH
UkITIFNMMSkwJwYDVQQDDCB2aWSDQXNpZ24gbmVidWxlbU1VJVEUyIEF1dGhvcml0eTAzFw0xOTA3
MTExMzU4NDJaFw0yNDA3MDkxMzU4NDJaMIG0MSowKAYDVQQDDCF2aW5lU0FzaWduIG5lYnVsYVNV
SVRFMSBBdXRob3JpdHkxEjAQBgNVBAsMCXZpbkNBc2lnbjEYMBYGA1UEYQwPVkEURVMtQyYyOTEz
OTI2MRUwEwYDVQQKDAxWSU5URUdSSVMgU0wxIDAeBgNVBAcMF0hPU1BJVEFMRVQgREUgTExPQUF
R0FUMRIwEAYDVQQIDAlCQVJDRUxPTkExCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAgirkD0wrkQNLD1CAeA5CGAHqH7hmQTQJWcdnKtVnRxtSdYs01LMLbFbiIF1
OSI+2RYroYMMORIpN2dJE7AKMBMbOHKabgWBlD9mJz/WTgbJg/RIBycVrpFNwhnX6tzDWNcc
3hjqcqoK3YmAkYOJKvJtmOX2GS7107keSBN7N9AeY68Wz4T0LvR/cTJLELyurJjX+3MhDD7CG8Xom
odjty+TUCsjqVnPrICScFWrlHMSqZMcnDdcNPTf6OopIzBQq5c6O8gzbZmbPiofIpNXJNtutzOo5
J7cQi8kwq5rttsjab/DIndnASgyWVpu1IxbFYIWNKDhG7F2W0DSZG/ZXzcEQvBRWaTbeNGK+UFxb
t7GHx89ErioWB/atzm5Za3HTWYYjHqHEeY5MEPgq/gwtQOxvka/6Z0ZDoGlGcBsLz7W2GsoET13m
5mp/KcIfs+nMDyAzt02gt4/YyRdhjIA8GY6LUAshxs8V9/0tzk35kZSYpv26QNZ38280A6QibEOWv
6B2OZLg41hdS8hpvh2femqhZp0XVsKO2xBxvZ1tnUjZxvq0m6xIe2CUwGaMCJPZGnZZms1K3XzXC
OcobhnVLYxo1djckPf8PpwTroAmpC9kvhJuTcblAq7fmBwDVs/wDLPNJ4QEh2/fLlwXhD2pp9DAk
BHr+UzRoi9TQjssCAwEAAaOCA14wggNaMHQGCCsGAQUFBwEBBGgwZjA9BggrBgEFBQcwAoYxaHR0
cDovL3dldy52aWSjYXNpZ24tbmV0L3B1Ymxp Y2tlcXMvY2FuZW11bGEyLmNydDAlBggrBgEFBQcw
AYYZaHR0cDovL29jc3AudmluY2FzaWduLm5ldDAdBgNVHQ4EFgQUk3OkzqC+eZYHLnMaQPni9kKw
luswDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRNInqGK5z2S3z32/pUUwvd9wVfjCBzgYIKwYB
BQUHAQMEgcEwgb4wCAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYEAI5GAQYwCQYHBACORgEGAjCB
jwYGBACORgEFMIGEMEAWOmh0dHBzOi8vd3d3LnZpbmNhc2lnbi5uZXQvcG9saWN5L2VuL1BEUy1U
U0EvcGRzLXRzYS1lbi5wZGYTAmVuMEAWOmh0dHBzOi8vd3d3LnZpbmNhc2lnbi5uZXQvcG9saWN5
L2VzL1BEUy1UU0EvcGRzLXRzYS1lcy5wZGYTAmVzMIHqBgNVHSAEgeIwgd8wgdEGCysGAQQBgvAz
AQkBMIHBMCgGCCsGAQUFBwIBFhxodHRwczovL3BvbGljeS52aW5jYXNpZ24ubmV0MIGUBggrBgEF
BQcCAjCBhwxBbENlcnRpZmlj YWRvIGNJYWxpZmlj YWRvIGNlYWxpZmlj YWRvIGRlIHNlbGxvIGVsZWN0csOzbmljbyBk
ZSBwZXJzb25hIGp1csOzCiljYSBwYXJhIGxhIGV4cGVkaWNpw7NuIGRlIHNlbGxvcyBjdWFsaWZp
Y2Fkb3MgZGUgdGllbXBvIGVsZWN0csOzbmljbzAJBgcEAIvsQAEBMGcGA1UdHwRgMF4wLaAroCmG
J2h0dHA6Ly9jcmwxLnZpbmNhc2lnbi5uZXQvY2FuZWJlbGEyLmNvbDAioCugKYYnaHR0cDovL2Ny
bDIudmluY2FzaWduLm5ldC9jYW5lYnVsYTIuY3JsMA4GA1UdDwEB wQEAwIGwDAWBgNVHSUBAf8E
DDAKBggrBgEFBQcDCDBFBgkqhkiG9w0BAQEEOAw2MjA0OC1CaXQgUHVibGljIGtlcSBlbmNvZGVk
IGluIGFjY29yZGFuY2Ugd2l0aCBSRkMzMjc5MA0GCSqGSIb3DQEBDQUAA4ICAQBB68NrieTNADPH
yabPXR8Kjg3JuasoZ0xceF0UwXUwPAXXyTaKKBf6a3+B/43753X3YjEen5PIAAyyn8N7Wc3GZGP
HDOtjU1MKlNhcZAvyVb4WMP3I1atlrsL0C4dY2uBkgd1DGBE8nC9ugxBpgpZ5TAVVFxaB8FTiW9
gp8omM8+tkQE1I53mMAODAW4lqkFtkN7D1NIlb/QEtOzHVLP1Yu2TF+K8THrLJGipoDXm6Xo
RWw1XFQiMz/Z/ZR7GKL/ooOhPY0xb1ntkyRMyMbsk/tvmqisvDv9OVaJ7ZwLiSOI46lXUnxQv9G
JPRKn0PC0PJTM0Gz4oHXjopTAq9FbTdv45/4cm9En03lWh+YtaJci0Ii3AV8QbYzUkJs5HgYd4TY
dEwIyQJWkqvs2T7BJesq+MtvsWIs0tb1YSLUrYt4ScoFjFM7B+Hcn1Ut8/T0CZPPpXnVHNCq4I6b
k+F9wpLCo1jsesxAEjv5MmIZQAtfwQW2Dza3kc5LHR+y2ryMUrdv3v/OZT62RPBj+LdUiPeZIZg8
XHjXtFi2V5qiRh115cR8O+CwMaYUU8RR2Qq+icdsVjuGtW3brvAof6+hwdmoAHz1mLEF9cY0QFt
n1rlCSbWzU/u/cW+BX/ZPJgodxOV5au2tH/6/Bte8VCE3EcMXl1wMe4oyK5VQQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *vinCAsign nebulaSUITE2 Authority*

Issuer O: *VINTEGRIS SL*

Issuer OU: *vinCAsign*

Issuer 2.5.4.97: *VATES-B62913926*

Issuer L: *HOSPITALET DE LLOBREGAT*

Issuer ST: *BARCELONA*

Issuer C: *ES*

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L:	*HOSPITALET DE LLOBREGAT*
Subject O:	*VINTEGRIS SL*
Subject 2.5.4.97:	*VATES-B62913926*
Subject OU:	*vinCAsign*
Subject CN:	*vinTSAsign nebulaSUITE1 Authority*
Valid from:	*Thu Jul 11 15:58:42 CEST 2019*
Valid to:	*Tue Jul 09 15:58:42 CEST 2024*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:82:3A:E4:0F:4C:2B:91:03:4B:0F:50:80:78:0E:42:18:01:EA:1F:B8:66:41:34:25:59:C7:67:2A:D5:7F:9D:1C:6D:49:D6:2C:D3:52:CC:2E:11:5B:8A:51:48:39:22:3E:D9:16:22:BF:36:0C:30:E4:48:A4:DD:9D:8C:4E:E2:00:A3:01:32:13:87:29:A6:E0:58:12:03:F6:62:33:FD:64:E0:84:98:3F:FD:12:01:C9:CF:D5:AE:91:4D:C2:19:D7:EA:B7:57:58:D7:9C:DE:18:EA:72:AA:0A:DD:89:80:91:83:89:2B:22:26:39:7D:86:4B:BD:74:EE:47:92:04:DE:CD:F4:07:98:EB:C5:B3:E1:3D:0B:BD:1F:DC:4C:92:C4:2F:2B:AB:26:35:FE:DC:C8:43:0F:B0:86:F1:7A:26:A1:D8:ED:CB:E4:D4:0A:C8:EA:56:73:EB:94:24:9C:15:6A:E5:1C:CE:6A:64:C7:27:0D:D7:0D:3D:37:FA:3A:8A:48:CC:14:2A:E5:CE:8E:F2:0C:DB:66:68:4F:8A:87:C8:A4:D5:C9:36:DB:AD:CC:EA:39:27:B7:10:8B:C9:30:AB:9A:ED:B6:C8:DA:6F:F0:C8:9D:D9:C0:E6:AC:96:36:9B:B5:23:16:C5:62:55:8D:28:38:46:EC:5D:96:D0:34:99:1B:F6:57:CD:C1:10:BC:14:56:69:36:DE:34:62:BE:50:5C:5B:B7:B1:87:C6:5F:44:AE:DA:16:07:F6:AD:CE:6E:59:6B:71:D3:59:86:23:1E:A1:C4:79:8E:4C:10:F8:2A:FE:0C:2D:41:0C:6F:91:AF:FA:67:46:43:A0:69:46:70:1B:0B:CF:B5:B6:1A:CA:04:4F:5D:E6:E6:6A:7F:29:C1:EC:FA:73:03:CB:8C:F4:DA:0B:78:FD:8C:8F:76:18:C8:03:C1:98:E8:B5:00:B2:1C:62:F1:5F:7F:D2:DC:E4:DF:99:19:49:8A:72:67:A4:2D:35:9D:FC:DB:CD:00:E9:08:A1:10:E5:AF:E8:1D:8E:64:B8:38:D6:17:7C:92:1A:6F:87:67:DE:9A:A8:59:A7:45:D5:B0:A3:B6:C4:1C:6F:67:5B:67:52:36:71:BE:AD:26:EB:12:1E:D9:C5:30:19:A3:02:24:F6:46:9D:96:66:B3:52:B7:5F:35:C2:39:CA:1B:86:75:4B:63:1A:35:76:37:A4:3D:FF:0F:A7:04:EB:A0:09:A9:0B:D9:2F:84:9B:93:79:B9:40:AB:B7:E6:07:00:D5:B3:FC:03:2C:F3:49:E1:01:21:DB:F7:CB:23:05:E1:0F:6A:69:F4:30:24:04:7A:FE:53:34:68:8B:D4:D0:8E:CB:02:03:01:00:01*
Authority Info Access	*http://www.vincasign.net/publickeys/canebula2.crt* *http://ocsp.vincasign.net*
Subject Key Identifier	*93:73:A4:CE:A0:BE:79:96:07:2E:73:1A:40:F9:E2:F6:42:B0:22:EB*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.47155.1.9.1* *CPS pointer: https://policy.vincasign.net* *CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]* *Policy OID: 0.4.0.194112.1.1*
CRL Distribution Points	*http://crl1.vincasign.net/canebula2.crl* *http://crl2.vincasign.net/canebula2.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*17:57:14:7A:3A:13:1C:C4:9C:FA:DE:37:4B:00:65:59:FB:A3:F0:EB:2D:9F:6A:4A:FF:41:DE:7B:2F:11:96:9D*

X509SubjectName

Subject C:	*ES*
Subject ST:	*BARCELONA*
Subject L:	*HOSPITALET DE LLOBREGAT*
Subject O:	*VINTEGRIS SL*
Subject 2.5.4.97:	*VATES-B62913926*
Subject OU:	*vinCAsign*
Subject CN:	*vinTSAsign nebulaSUITE1 Authority*

X509SKI

X509 SK I	*k3OkzqC+eZYHLnMaQPni9kKwIus=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2019-08-02T00:00:00Z*

27.5 - Service (granted): Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE2 Authority

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[es]*	*Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE2 Authority*
Name	*[en]*	*Qualified time stamps issued by vinTSAsign nebulaSUITE2 Authority*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*1601373709008309851*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJSzCCBzOgAwIBAgIIFjk452YXDlswDQYJKoZIhvcNAQENBQAwgbMxCzAJBgNVBAYTAkVTMRIw
EAYDVQQDDAlCQVJDRUsPTkEsIDAeBgNVBAcMF0hPU1BJVEFMRVQgREUgTExPQUFR0IUMRgwFgYD
VQRbDA9WQVRFUy1ICNj5MTM5MjYxEjAQBgNVBAsMCXZphkNBc2lnbjEYMBMGA1UECgwMVkltOYEVH
UkITIFNMMSkwJwYDVQQDDCB2aWSDQXNpZ24gbmVidWxhU1VJVEUyIEF1dGhvcml0eTAeFw0xOTA3
MTExNDQ0NTFaFw0yNDA3MDkxNDQ0NTFaMIG0MSowKAYDVQQDDCF2aWSU0FzaWduIGSlYnVsYVNV
SVRFMiBBdXRob3JpdHkxEjAQBgNVBAsMCXZphkNBc2lnbjEYMBYGA1UEYQwPVkFURVMzOTEz
OTI2MRUwEwYDVQQKDAxWSU5URUdSSVMgU0wxIDAeBgNVBAcMF0hPU1BJVEFMRVQgREUgTExPQUF
R0FUMRIwEAYDVQQIDAlCQVJDRUsPTkExCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAzqsFyzeeiJLANlmFUhEYcDGjdJHI3BDxYEZyMs32KlZm/lmPuCmNwpNjmSoO
skBh1L9ZRlzwhWOt7LjJn76gevd4Zxicyo6CbtF70tc2LbGrObHPq0phKAWV6ezFiGmzYVmgZACi
z4gUIlwXCtzX+6d6SAgY1Bmul3gF1/uS7iHGNgm60gWVTA3gramUCwIyUZImBCCYVdquoIDCBz
/BD8kMy4g/8P7vLq0Pmn3stFw5bVS9mRQ3JuoBlx3JXMhc3zqJZ6dYK3NQsvmvboSKl6+Fxb5I/
+zNo+OL7gEg90mE9CLJWLDClvkTdfRWvCWIFupG+4GEc+Q9aSRR6DzkawBTI6mL6kQb+ZQUUku0s
+0G5kkSJL9Hfu+LVwt8OU3tA0lQ8jqhoT3a2xPFI9Tw/fss1Usu0SPPqZ+PaXre6MzFZExNvhfc/
ihHC56GkzE21J81/RHvEDmBuMWW/cPAcMrKHPROvWpXthvTXIWOgBHU2E6zHGBs5K/9yRuPO/S
UeYUkjnd4jOhlajsHf5F6vlFVtpZqGgayQvikrH2E3Ci0oJfdcNUHgQ/PkNUs/B5XSu2QXE7EjuP
8VdOL8NS66QlUw0lDpVrOB8cQWettTKF/aR9mc5ixfMSfTbOyb2N6z9JplmYp3fvEg8i6P6gTLQro
3yq/IOButOxKy2cCAwEAAaOCA14wggNaMHQGCCsGAQUFBwEBBGgwZjA9BggrBgEFBQcwAoYxaHR0
cDovL3dfy5ZaWSjYXNpZ24ubmV0L3B1YmxpY2tlcXMvY2FuZWJ1bGEyLmNydDAfBggrBgEFBQcw
AYYZaHR0cDovL29jc3AudmluY2FzaWduLmS0dDAdBgNVHQ4EFgQU8B2lW2cFmuzBIPYu9DiMOw+7
gTIwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRN1nqGK5z2S3r32/3pUUwvd9wWfjCBzgYIKwYB
BQUHAQMEgcEwgb4wCAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYEAI5GAQYwCQYHBACORgEGAjCB
jwYGBACORgEFMIGEMEAWOmhtdHBzOi8vd3d3LnZpbmNhc2lnbi5uZXQvcG9saWN5L2VuL1BEUy1U
U0EvcGRzLXRzYS1lbi5wZGYTAmVuMEAWOmhtdHBzOi8vd3d3LnZpbmNhc2lnbi5uZXQvcG9saWN5
L2VzL1BEUy1UU0EvcGRzLXRzYS1lcy5wZGYTAmVzMIHqBgNVHSAEgelwgd8wgdEGCysGAQQBgvAz
AQkBMIHBMCgGCCsGAQUFBwIBFhxodHRwczovL3BvbGljeS52aW5jYXNpZ24ubmV0MIGUBggrBgEF
BQcCAjCBhwyBhENlcnRpZmlj YWRvIGN1YWxpZmlj YWRvIGRlIHNlbGxvIGVsZWN0csOzbmljbyBk
ZSBwZXJzb25hIGp1csOzZGlj YSBwYXJhIGxhIGV4cGVkaWNpw7Nu1GRlIHNlbGxvcyBjdWFsaWZp
Y2Fkb3MgZGUgdGllbXBvIGVsZWN0csOzbmljbzAJBgcEAIvsQAEBMGcGA1UdHwRgMF4wLaAroCmG
J2h0dHA6Ly9jcmwxLnZpbmNhc2lnbi5uZXQvY2FuZWJ1bGEyLmNybDAtoCugKYYnaHR0cDovL2Ny
bDIudmluY2FzaWduLmS0dC9jYW5lYnVsYTIuY3JsMA4GA1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8E
DDAKBggrBgEFBQcDCDBFBgkqhkiG9w0BAQEECDAw2MjA0OC1CaXQgUHVibGljIGlzSBbmNvZGVk
IGluIGFjY29yZGFuY2UgdZI0aCBSRkMzMjc5MA0GCSqGSIb3DQEBDQUAA4ICAQCWbGF1MGysRFpJ
DJcoYWOo5w76IjskqP4lhBaTasElF3HnZYK5ccZmwcGcHZYhsfgN9pwptcMCRZgcKGzO61V17bsA
81canFUUUPSQui0xSpy8/3L kisDEokCnKeTDX5lSymxE36Fd9i1VlEg9mBHFBBk38Kcir1jcXUp
1frKXcCF2YeKz4uSf5xIkV1nKVCUmj1ZATF+3c4sdy22nqnzEtBgIB3cE2VIOOK/ETxIO9E/sYdn
mpmBhU/08qIbA71BbRr3dxt56FdtxAVPvOdsOXX+Yd5afyxWl4L6Od+hmUAyCgeMOqjIY6xwO1eYV
ADkSl7kH+jjgjl/W2gMN2qnAsWEuIFY95LgavEvGoguBpHt5hmRLwf59tkXCZ0alK02QJT71juJ
ZppRgJeSNCEFFBCzpOpelttiIEiOcIm8xKHGPGcsd254OTI3QJRYq0tdEFx8gMqMvIVnQ+MG4Mje
oarAf01ee8bvA1+UgMeZKxOuSly3ZG2Gow1xSFaVZ0aqoeLSjVwSzibT1uF5Mdi/6/W5F+isEaw5
ImoM+eQtR1OEliQP1ttOZy+EqUUq0vWSGc4AO0GHMCndWqVLYDyoJF8lLKwBxFN5I4/kjyqhbyK
FMGg7kmR8WXZd6HIIzjQi6BAden8NuFW9glzGcW2ApdcjrT3p1cA7fiP3Tpalg==

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: *vinCAsign nebulaSUITE2 Authority*

Issuer O: *VINTEGRIS SL*

Issuer OU: *vinCAsign*

Issuer 2.5.4.97: *VATES-B62913926*

Issuer L: *HOSPITALET DE LLOBREGAT*

Issuer ST: *BARCELONA*

Issuer C: *ES*

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SL*

Subject 2.5.4.97: *VATES-B62913926*

Subject OU: *vinCAsign*

Subject CN: *vinTSAsign nebulaSUITE2 Authority*

Valid from: *Thu Jul 11 16:44:51 CEST 2019*

Valid to: *Tue Jul 09 16:44:51 CEST 2024*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CE:AB:05:CB:37:9E:88:92:C0:34:89:85:52:11:18:70:31:A3:74:91:C8:DC:10:F1:60:46:72:32:CD:F6:2A:56:66:FE:59:
8F:B8:29:8D:C2:93:63:99:2A:0E:B2:40:61:D4:BF:59:44:8C:F0:85:63:A2:EC:B8:C8:9F:BE:A0:7A:F7:78:67:18:9C:CB:A0:9B:B4:57:FB:D1:ED:8B:6C:6A:CE:6C:73:EA:D2:98:51:01:65:7A:7B:31:5F:1B:39:F3:61:59:A0:64:
00:A2:CF:88:14:B4:8C:17:0A:2C:D7:FB:A7:7A:48:08:18:D4:19:EE:20:91:A0:17:F2:F2:89:2E:E2:1C:63:60:9B:AD:20:59:54:C0:DE:0A:DA:99:40:B0:D7:25:19:22:60:42:0A:D5:5D:82:EA:1F:0C:20:73:FC:10:FC:90:CC:B8:8
3:FF:0F:EE:F2:EA:D0:F9:A7:DE:C8:AD:17:0E:5B:55:2F:66:45:0D:C9:BA:80:65:C7:72:57:32:17:37:CE:AD:59:E9:D6:0A:DC:D4:2C:BE:6B:DB:A1:22:A5:EB:E1:71:6F:99:7F:FB:33:68:F8:E2:FB:80:48:3D:D2:61:3D:08:B2
:56:2C:30:A5:BE:44:DD:7D:15:AF:09:69:45:BA:91:BE:E0:61:1C:F9:0F:5A:49:14:7A:0F:39:1A:C0:14:E5:EA:62:FA:91:06:FE:65:05:14:92:ED:2C:FB:41:B9:92:44:89:2F:D1:FA:BB:E2:D5:C2:DF:0E:53:7B:40:D2:54:3C:8E:
A8:68:4F:76:B6:C4:F1:48:F5:3C:3F:7E:CB:13:53:1B:B4:48:F3:EA:67:E3:DA:5E:B7:BA:33:31:59:13:13:6F:85:F7:3F:8A:11:C2:4B:A1:A4:CC:4D:B5:27:CD:7F:44:7B:C4:0E:60:6E:31:65:BF:7B:F3:C0:78:CA:CA:1C:F4:4E:
BD:6A:57:B6:1B:D3:5C:85:8E:80:11:D4:D8:4E:B3:1C:60:6C:E4:A8:FD:C9:18:A2:3C:EF:D2:51:E6:14:92:39:DD:E2:33:A1:21:A8:EC:1D:FB:05:EA:F9:45:56:DA:59:A8:68:1A:C9:0B:E2:2A:B1:F6:13:70:A2:D2:82:5F:75:C
3:54:1E:04:3F:3E:43:54:8B:F0:79:5D:2B:B6:41:71:3B:12:3B:8F:F1:57:4E:2F:C3:52:E9:09:54:C3:49:43:A5:5A:CE:07:C7:10:59:EB:5F:4E:41:7F:69:1F:66:73:98:B1:7C:C4:9F:4D:B3:B2:6F:63:7A:CF:D2:69:22:66:29:DD:FB:
C4:83:C8:BA:3F:A8:13:2D:0A:E8:DF:2A:BF:94:E0:6E:B4:EC:4A:CB:67:02:03:01:00:01

Authority Info Access	*http://www.vincasign.net/publickeys/canebula2.crt* *http://ocsp.vincasign.net*
Subject Key Identifier	*F0:1D:A5:5B:67:05:9E:EC:C1:20:F6:2E:F4:38:8C:3B:0F:BB:81:32*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.47155.1.9.1* *CPS pointer: https://policy.vincasign.net* *CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]* *Policy OID: 0.4.0.194112.1.1*
CRL Distribution Points	*http://crl1.vincasign.net/canebula2.crl* *http://crl2.vincasign.net/canebula2.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*FB:75:52:A8:36:0A:2D:4D:89:4B:F3:8C:4E:B4:A6:A0:9C:8E:CF:1E:25:C5:4F:B1:E2:02:D1:85:76:61:3A:51*

X509SubjectName

Subject C:	*ES*
Subject ST:	*BARCELONA*
Subject L:	*HOSPITALET DE LLOBREGAT*
Subject O:	*VINTEGRIS SL*
Subject 2.5.4.97:	*VATES-B62913926*
Subject OU:	*vinCAsign*
Subject CN:	*vinTSAsign nebulaSUITE2 Authority*

X509SKI

X509 SK I	*8B2lW2cFnuzBIPYu9DiMOw+7gTI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2019-08-02T00:00:00Z

27.6 - Service (granted): Qualified Certificates issued by vinCAsign nebulaSUITE4 Authority

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by vinCAsign nebulaSUITE4 Authority*

Name *[es]* *Certificados Cualificados emitidos por vinCAsign nebulaSUITE4 Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *592846264893196737726411358607176543381952486368*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHqjCCBZKgAwIBAgIUZ9glXDhZfSM5jEZWVLNECiWVW+AwDQYJKoZIhvcNAQENBQAwgZ0xCzAJ
BgNVBAYTAkVTMRYwFAYDVQQKDAJWw61udGVncmlzIFNMMSAwHgYDVQQHDBdlb3NwaXRhbGV0lGRl
lExsb2JyZWdhdDEYMBYGA1UEYQwPVkFURVMtQjYyOTEzOTI2MSYwJAYDVQQDDB12aWSDQXNpZ24g
UXVhbGlmaWVkIEF1dGhvcmI0eTESMBAGA1UECAwJQmFyY2Vsb2ShMB4XDTIwMDUwODExMTk0OFoX
DTMzMDUwODExMTk0OFowgbMxC2AJBgNVBAYTAkVTMRIwEAYDVQQIDAlCQVJDRUxPTkExIDAeBgNV
BAcMF0hPU1BJVEFMRVQgREUgTExPQUFR0FUMRgwFgYDVQRhDA9WQVRFUy1CNjI5MTM5MjYxEjAQ
BgNVBAsMCXZpbkNBc2lnbjEVMBMGA1UECgwMVkIOVE VHUkITIFNMMSkwJwYDVQQDDCB2aWSDQXNp
Z24gbmVidWxhU1VVEU0lEF1dGhvcmI0eTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
AMf6gcXmS/kX32woSpcKvCEIcQSZ1VRCspsXXkP2dGX9R06QhRZEuL10w4K5lYFp4RYlazzpzI
5u5lunAuxLQnfU29Os0WxHbMnfsSHIMAYpCAbW/cEm7k4WinMBtdw+ksBOTGHjBZQ1Py73UoN33m
UNegfyI7lOvlvrnBomMNFnLtN5TvHkN0gLlWrrKwfSZa0/pOOIVJek0vJypkdLwjrVIxmlgl5ViZ
+qbxFRb4HBlBkWjvMwYC5O6v7o4nT1QPqSQ7xzWzl3d9kEsQkarJtEW72p8R5eN1opOctKB+oEzf
n680wCbd9x1VFIqKaCdkuZ+Pwcg9uVSw7qk0qtW+D2y9Bb0b46mVrYisM4IQ0b26bMR47ONb7Xc4
z6wU0EEhyYPOlDH8cP8DoOr+a0kcZbgITDN9IXUBLopituwXRgAHJWLlseuVQehLLqqQpj0a/ldw
IO5rAPtE1ogrRNlmZCpMXD97NOaxIBkJAljzPlSUzxjaaZLMvSCd+Z6XK0SJ1p4JhldpkEFIXz2R
DgcDBdXvIw6bR0L4ZA+REPuJ4bcf62/XAP62uzroT6fu9ZVIZVngcv/a5hizCsYuMNCnnB/v3kq1
yBUZ/tO94g6CmKuNP9gfugz2c9NTUn3IaIDzD+IudIu6zJ59IAzcBfgu3rMJbkYmQJWuINQdpRmV
AgMBAAGjggHIMIIBxDAfBgNVHSMEGDAWgBTQPkpqkm9Ns4ZHXHTkVqMC9Bhl0DAdBgNVHQ4EFgQU
o+c+fRSSt3Ur8GiWzHhEgJfuLgMwDgYDVR0PAQH/BAQDAgEGMIGMBgNVHSAEgYQwgYEwfwYEVR0g
ADB3MCgGCCsGAQUFBwIBFhxodHRwczovL3BvbGljeS2aW5jYXNpZ24ubmV0MEsGCCsGAQUFBwIC
MD8MPUNlcnRpZmlyYWRvIENBIFN1Ym9yZGlnYWRhLiBWZXIgIGlhbdHBzOi8vcG9saWN5LnZpbmNh
c2tnbi5uZXQwHQYDVR0RBBYwFIESaW5nb0B2aW5jYXNpZ24ubmV0MF8GA1UdIwRYMFYwKaAnoCWG
I2h0dHA6L y9jcmwzLnZpbmNhc2lnbi5uZXQvY2FzdWluY3JsMCmgJ6AlhiNodHRwOi8vY3JsNC52
aW5jYXNpZ24ubmV0L2Nhc3ViLmNybDBPBggrBgEFBQcBAQRDMEEwPwYIKwYBBQUHMAKGM2h0dHA6
Ly93d3cudmluY2FzaWduLm5ldC9wdWJsaWNzXZIzL2NhcXVhbGlmaWVkLmNlcjASBgNVHRMBAf8E
CDAGAQH/AgEBMA0GCSqGSIb3DQEBDQUAA4ICAQAfQscYg4Tnv5RVm/WUmfhbAAX8OLJnskuk6RT2S
FUdyiniHSnij/bjKz14BbLGORmfLR16NabuSb5IZ+MT+1TrZacSLdYPTpNn22fVcsQaPaYIBWhzL
lRsMfmoCtP2c6s4JAPQRR0LpBBr0h5EWqxUwupseWJn8Or1OSvQgUPYlR39BCjFOg22PczUW9JQx
yS3CR0+UWRAh/x2MdDNHMT1yFdB7tI1Ns26tzCs0sE6zwLOGlkXuF/bXMZXQRLFoxJB26ayht9pN
NWCYt2mYrqvvuWxST8AvSPDXJmXcXoYVg2G+/XaoPEJTOxH9g8bsxKX3GcgGn72bH1AWwwOUlb+cYg
eXsG+wDN6Ul h9yxyTDazSR9qvH0lO+5IU8okIQE0giEQGis5onRM7sXw5+A1wrXYAfgsgUiD8yHNc
7XS8NRqxabzL9kZXb6LfMjRiu9lW515SnWvVSlGriP7qhl3fXDlAuboUWtEyts+M8Le/vb24X0YG/
nrcA3KqQAoVp1mygSmX+8pIf+7VoqTu1VPta/V58s5TLqjV+ryGHNqsOHouRNc60n2Oa3o5e8f6Sr
1RgaV0h9pml4y1OsB8yz3jscDAF15L7HKcIfzRoKzS8xB7WW4S+oMRmPuhs5Gi8mY2TUkq2L7ar
1edmjiW2pCTnqZZO8zGYMiuqZZF3jfIssPzTA==

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer ST: *Barcelona*

Issuer CN: *vinCAsign Qualified Authority*

Issuer 2.5.4.97: *VATES-B62913926*

Issuer L: *Hospitalet de Llobregat*

Issuer O:	*Víntegris SL*
Issuer C:	*ES*
Subject CN:	*vinCAsign nebulaSUITE4 Authority*
Subject O:	*VINTEGRIS SL*
Subject OU:	*vinCAsign*
Subject 2.5.4.97:	*VATES-B62913926*
Subject L:	*HOSPITALET DE LLOBREGAT*
Subject ST:	*BARCELONA*
Subject C:	*ES*
Valid from:	*Fri May 08 13:19:48 CEST 2020*
Valid to:	*Sun May 08 13:19:48 CEST 2033*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C8:BC:81:E5:E6:48:8B:CA:5F:7D:B0:A2:24:A9:BC:AB:C2:10:97:10:49:9D:55:44:2B:29:49:75:E4:3F:67:46:5F:D4:4E:E9:08:91:64:4B:8B:D7:4C:38:2B:99:58:16:9E:11:62:56:B3:CE:3C:C8:E6:EE:65:BA:70:2E:C4:B4:27:7D:4D:BD:3A:CD:16:C4:76:CC:9D:FB:12:1C:83:00:62:90:80:6D:6F:DC:12:6E:E4:E1:68:A7:30:1B:5D:C3:E9:2C:04:E4:C6:1E:30:59:43:53:F2:EF:75:28:37:7D:E6:50:D7:A0:7F:22:3B:94:EB:E5:BE:B9:C1:A2:63:0D:16:72:ED:37:94:EF:1E:43:74:80:B9:56:AE:B2:B0:7D:26:5A:D3:FA:4E:38:85:49:7A:4D:2F:27:2A:64:74:BC:23:AD:52:31:98:88:25:E5:58:99:FA:A6:F1:15:16:F8:1C:17:C1:91:68:EF:33:06:02:E4:EE:AF:EE:8E:27:4E:D4:0F:A9:24:3B:C7:35:B3:97:77:7D:90:4B:10:91:AA:C9:88:45:BB:DA:9E:11:E5:E3:75:A2:93:9C:B4:A0:7E:A0:4C:DE:9F:AF:34:C0:28:78:F7:1D:55:16:5A:8A:68:E7:64:BB:F6:7E:3F:07:20:F6:E5:52:C3:BA:A4:D2:AB:56:F8:3D:B2:F4:18:74:87:8E:A6:56:76:22:B0:CE:08:43:48:76:E8:C4:78:EC:E3:61:ED:77:38:CF:AC:14:D0:41:21:C9:83:CE:94:31:FC:70:FF:03:A0:E8:BE:6B:49:1E:65:B8:08:4C:33:7D:95:75:01:2E:8A:62:B6:EC:17:46:00:07:25:62:E5:B1:EB:95:41:E8:4B:2E:AA:90:A6:3D:1A:FE:57:70:20:EE:6B:00:FB:44:D6:88:2B:44:D2:26:64:2A:4C:5C:3F:7B:34:E6:B1:20:19:09:02:58:F3:3E:54:94:CF:18:DA:69:92:CC:BD:20:9D:F9:9E:97:2B:44:89:D6:9E:09:86:57:69:90:41:48:5F:3D:91:0E:07:03:05:D5:EF:23:0E:A1:47:42:F8:64:0F:91:10:FB:89:E1:B7:1F:EB:6F:D7:00:FE:B6:BB:3A:E8:4F:A7:EE:F5:95:48:65:59:E0:72:FF:DA:E6:18:B3:0A:C6:2E:30:D0:A7:9C:1F:EF:DE:4A:B5:C8:15:19:FE:D3:BD:E2:0E:82:98:AB:8D:3F:D8:1F:B6:E8:22:D9:CF:4D:4D:49:F7:21:A0:D9:0F:E2:2D:76:5B:BA:CC:9E:7D:24:0A:DC:06:58:2E:DE:B3:09:86:46:26:40:95:AE:7C:D4:1D:A5:19:95:02:03:01:00:01*
Authority Key Identifier	*D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0*
Subject Key Identifier	*A3:E7:BE:7D:14:92:B7:75:2B:F0:68:96:CC:78:44:80:97:EE:2E:03*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.vincasign.net* *CPS text: [Certificado CA Subordinada. Ver https://policy.vincasign.net]*
Subject Alternative Name	*info@vincasign.net*
CRL Distribution Points	*http://crl3.vincasign.net/casub.crl* *http://crl4.vincasign.net/casub.crl*
Authority Info Access	*http://www.vincasign.net/publickeys/caqualified.cer*
Basic Constraints	*IsCA: true - Path length: 1*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1C:A3:C0:A2:84:F8:94:DB:A0:A9:7C:83:53:1E:8C:06:2D:1D:54:F6:E7:F9:66:FA:32:3E:52:8E:F7:B9:B8:47*

X509SubjectName

Subject CN:	*vinCAsign nebulaSUITE4 Authority*
Subject O:	*VINTEGRIS SL*
Subject OU:	*vinCAsign*
Subject 2.5.4.97:	*VATES-B62913926*
Subject L:	*HOSPITALET DE LLOBREGAT*
Subject ST:	*BARCELONA*
Subject C:	*ES*

X509SKI

X509 SK I	*o+e+fRSSt3Ur8GiWzHhEgJfuLgM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-11-18T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

27.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

27.7 - Service (granted): Qualified Certificates issued by vinCAsign nebulaSUITE5 Authority

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by vinCAsign nebulaSUITE5 Authority*

Name *[es]* *Certificados cualificados emitidos por vinCAsign nebulaSUITE5 Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *652595285322423139354080566802658888035528036396*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHyTCCBbGgAwIBAgIUck9eiymg8t1HNxcD38uS+VvUCwwDQYJKoZIhvcNAQENBQAwgZ0xCzAJ
BgNVBAYTAkVTMRYwFAYDVQQKDA1Ww61udGVncmlzIFNMMSAwHgYDVQQHDBdlb3NwaXRhbGV0IGRl
IExsb2JyZWdhdDEYMBYGA1UEYQwPVkFURVMtQjYyOTEzOTI2MSYwJAYDVQQDDB12aW5DQXNpZ24g
UXVhbGlmaWVkIEF1dGhvcmI0eTESMBAGA1UECAwJQmFyY2Vsb25hMB4XDTIwMTExMTE1NDYxNVoX
DTMzMTExMTE1NDYxNVowgbMxC2AJBgNVBAYTAkVTMRIwEAYDVQQIDAlCQVJDRUxPTkEsIDAzBgNV
BAcMF0hPU1BJVEFMRVQgREUgTExPQUFR0FUMRgwFgYDVQRhDA9WQVRFUy1CNj15MTM5MjYxEjAQ
BgNVBAsMCXZpbkNBc2lnbjEVMBMGA1UECgwMVkIOVE VHUkITIFNMMSkwJwYDVQQDDCB2aW5DQXNp
Z24gbmVidWxhU1VVEU1HEF1dGhvcmI0eTCCAIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
AKFm/ZGMhJEma8HVK17Yx3lBkgNkTLNmFPGXzF8NmXk0tgfloWyIKbcujeGcBM32q0cOAE+rK/uZs
t2NYAT7KO63ghZd28bMLeKalCcFhjd6uotsTzYQUl8l9vZwLGKJsgYBRRXzr+ZAD1bfewNCZzrVH
+92scJg46TSLO7GSmRnimoxy4zjcpv4el57Kc1/YFBEU9AtyX1pivuGYh1ThNNyrUAJrbR0s3VT3
u8KGamMdM5Dguo7selySfFp9ngm+8K9eVPc2dCvCxMqvyiodUCnHUhIKgmXal1DVV5gbsWVObQIJ
0tMk95YcdYQm33NvtcS6tlJaDXiFsWDxBF77b8IzJ+SbTOXXL3OFtzNWCmZgdG4dunoks90JA
bewa5/4h2gkuIr4+HXVVI2DFhMBjY+RhoRgyOQRUE0tuW6LYvr/kMy+noT5/Gx86rKel7NfkXGK
eGqdTw8kNTI0miQCh26/CDpwoOwR2zF3CC49HAsFHC3wyfgK9sF2LbR4iq/Y19k8AsZGx7ROOx/2
s8BjMn7q3pcuZpLvjUBc3s9Jfm0XlNaQqn0DqGFpnsZOzJYDBXGnmLXk79iOpMGaaIge14ZyfT9
+PsQKRK7t0bIlP/RF4VMj19ER+XH9cx0NNDwBMI0t4X3hLPpdqFuB1VL2nay9RIfx0UGgZJ6GYz
AgMBAAGjggHnMIIB4zAfBgNVHSMEGDAWgBTQPkpqkm9Ns4ZHXH7kVqMC9Bbl0DAdBgNVHQ4EFgQU
KbCjxnlrKo2fWDWssfwk2n6SfBEwDgYDVR0PAQH/BAQDAgEGMIGMBgNVHSAEgYQwgYEwfwYEVR0g
ADB3MCgGCCsGAQUFBwIBFhxodHRwczovL3BvbGljeS52aW5jYXNpZ24ubm V0MEsGCCsGAQUFBwIC
MD8MPUNlcnRpZmlyYWRvIENBIFN1Ym9yZGluYWRhLiBWZXIgIGb0dHBzOi8vcG9saWN5LnZpbmNh
c2Nnbi5uZXQwHQYDVR0RBBYwFIESaW5mb0B2aW5jYXNpZ24ubm V0MF8GA1UdIwRYMFYwKaAnoCWG
I2h0dHA6L y9jcmwzLnZpbmNhc2lnbi5uZXQvY2FzdWluY3JsMCmgJ6AlhiNodHRwOi8vY3JsNC52
aW5jYXNpZ24ubmV0L2Nhc3ViLmNybDBPBggrBgEFBQcBAQRDMEEwPwYIKwYBBQUHMAKGM2h0dHA6
Ly93d3cudmluY2FzaWduLm5ldC9wdW3saWNzZXIzL2NhcXVhbGlmaWVkLmNlcjASBgNVHRMBAf8E
CDAGAQH/AgEBMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQ0FAAOC
AgEAI21e65nVVoBTE4LXA4ndNF9z+mcnp1/d5qciMTc8JVN0dxVFGDAzc6o0FKC7A2oxyK4CQ1Xa
qHzLXcqB+SXvkzPFCX4NuFcsoIk9x9w4ilS7fL lnDjpHjMD32gyctWzvDlALezVDiBgk+6GzfgZ5
imoC1o4N2fAVZwEIAcJRZEzdOg9PkwyBOCwmsa0lYansLmFdCOVYJ50lhJOlRPh2KGNbQbzG+KJ1
McjOzrH4pmj63tcmOPF6je9baE3HFZZwEKZLDasQjf1pQSGSdgg1y7VUyaX6EHp7+5ZZpA
T6FNPBkaahGrXssouGjjU/m9+0HcUdNfhN5WU62A2Qe4eeF/XaGYh+GJhRa/g346OcxagHi19KxB
Pgfb5shvLQlhsoY8O/HI228t5IN6sYdnLAgZyQEa6fjaVHDRIbUx0Pgp3hqZ9BuYE1YrlvSPQ3k1
YlQiQq8wXQFSovq7uB8qRf7UP3p2FHIXeE4TH8kJke+p8QVivCYioBNl8nXod7SmVz6qSbOEy1hK
ZXQ2YAAgWuhaOptv9+mYy9T0aqL/4nBWZT3Lc+S1vzjs9NmusgYvAqLtpHI7kOW20lYsduYj2p
mrUAiCasKXg10ykhMzsoV/ND0oFkDFWyNRUczxDzfqWxkPuxoiUzg4kk4c8zhL4REFuKxyJg+cm
+PM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer ST: *Barcelona*

Issuer CN: *vinCAsign Qualified Authority*

Issuer 2.5.4.97: *VATES-B62913926*

Issuer L: *Hospitalet de Llobregat*

Issuer O: *Víntegris SL*

Issuer C: *ES*

Subject CN: *vinCAsign nebulaSUITE5 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

Valid from: *Wed Nov 11 16:46:15 CET 2020*

Valid to: *Fri Nov 11 16:46:15 CET 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A1:66:FD:91:8C:84:41:26:6B:C1:D5:2B:5E:D8:BF:79:41:6A:03:64:4C:B3:66:14:F1:97:CC:5F:0D:99:79:34:81:F9:68:5B:2D:4A:6D:EB:A3:78:67:01:33:7D:AA:D1:C3:80:13:EA:CA:FE:E6:6C:B7:63:58:01:3E:CA:3B:AD:E0:85:97:76:F1:B3:0B:78:A6:A5:09:C1:65:8A:37:7A:BA:8B:6C:4F:36:10:53:C9:7D:BD:9C:0B:18:A2:6C:81:80:51:45:7C:EB:F9:90:03:D5:B7:DE:C0:D0:99:CE:B5:47:FB:DD:AC:78:98:38:E9:3E:4B:3B:B1:92:99:19:E2:9A:8C:72:E3:38:DC:A6:FE:1C:97:9E:CA:73:5F:D8:14:11:14:F4:0B:72:5F:5A:62:BE:E1:98:87:54:E1:34:DC:AB:50:02:6B:6D:1D:2C:DD:54:F7:BB:C2:86:6A:63:1D:33:90:E0:BA:8E:EC:78:8C:92:B4:5A:7D:9E:09:BE:F0:AF:6B:54:F7:36:74:2B:C2:C4:CA:AF:CA:2A:1D:50:29:C7:50:79:4A:82:65:DA:97:50:D5:57:98:1B:B1:65:4E:6D:02:09:D1:F3:24:F7:96:1C:76:26:10:9B:7D:CD:BE:D7:12:E8:12:48:68:35:E2:16:85:83:C4:11:7B:ED:BF:21:AC:9C:FE:E5:B4:CE:5D:72:F7:38:5B:6B:35:60:AB:9D:98:1D:1B:47:6E:C2:4B:3D:D0:99:40:6D:EC:1A:E7:FE:21:DA:09:2E:26:BE:3E:1D:75:55:22:2D:83:16:13:01:8D:8F:91:86:84:60:C8:E4:11:50:4D:2D:B9:6E:8B:62:FA:FF:90:CC:BE:9E:84:F9:FC:6C:7C:EA:B2:9E:23:B3:5F:91:71:8A:78:6A:9D:4F:0F:24:35:32:34:9E:24:02:87:6E:BF:08:3A:70:A0:EC:11:DB:31:77:08:2E:3D:1C:0B:05:1C:2D:F0:C9:F8:0A:F6:C1:76:2D:B4:78:8A:AF:D8:D7:D9:3C:02:C6:46:C7:B4:4E:3B:1F:F6:B3:C0:63:32:7E:EA:DE:97:2E:66:92:EF:8D:40:5C:DE:CF:49:7E:6D:17:20:D6:90:AA:7D:03:B8:61:69:9E:C6:4E:CC:98:D8:0C:15:C6:9E:62:D7:93:BF:62:3A:93:06:69:A9:60:7B:5E:19:C9:F4:FD:F8:FC:50:29:12:BF:AF:46:E5:D0:FF:D1:17:FE:15:32:3D:7D:11:1F:97:07:DA:31:D0:D3:43:C0:13:1F:97:4E:17:DE:12:CF:A5:DA:85:B8:1D:55:2F:69:DA:CB:D4:65:23:1D:14:1A:06:49:E8:E6:33:02:03:01:00:01

Authority Key Identifier *D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0*

Subject Key Identifier *29:B0:A3:C6:79:6B:2A:8D:9F:58:35:AC:B1:FC:24:DA:7E:92:7C:11*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://policy.vincasign.net

CPS text: [Certificado CA Subordinada. Ver https://policy.vincasign.net]

Subject Alternative Name *info@vincasign.net*

CRL Distribution Points

http://crl3.vincasign.net/casub.crl

http://crl4.vincasign.net/casub.crl

Authority Info Access *http://www.vincasign.net/publickeys/caqualified.cer*

Basic Constraints *IsCA: true - Path length: 1*

Extended Key Usage *id_kp_serverAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AA:AF:2F:29:EF:52:44:71:CB:4F:15:B7:2D:E6:A5:54:26:29:97:8F:B5:A9:14:A6:11:95:5C:75:AE:5E:F3:C3*

X509SubjectName

Subject CN: *vinCAsign nebulaSUITE5 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *KbCjxnlrKo2fWDWssfwk2n6SfBE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-01-26T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

27.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

28 - TSP: ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

.

TSP Name

Name	*[en]*	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*
Name	*[es]*	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*

TSP Trade Name

Name	*[en]*	*esFIRMA*
Name	*[es]*	*esFIRMA*
Name	*[en]*	*VATES-A50878842*
Name	*[en]*	*AULOCE S.A.U.*
Name	*[en]*	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*
Name	*[en]*	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

PostalAddress

Street Address	*[en]*	*Calle Bari 39 (Edificio Binary Building)*
Locality	*[en]*	*Zaragoza*
State Or Province	*[en]*	*Zaragoza*
Postal Code	*[en]*	*50197*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Calle Bari 39 (Edificio Binary Building)*
Locality	*[es]*	*Zaragoza*
State Or Province	*[es]*	*Zaragoza*
Postal Code	*[es]*	*50197*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*http://www.esfirma.com*

URI	*[en]*	*mailto:info@esfirma.com*
URI	*[es]*	*mailto:info@esfirma.com*
URI	*[es]*	*http://www.esfirma.com*

TSP Information URI

URI	*[en]*	*https://esfirma.com/doc-pki/index-ES.html*
URI	*[es]*	*https://esfirma.com/doc-pki/index-ES.html*

28.1 - Service (withdrawn): Qualified Certificates issued by ESFIRMA AC AAPP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by ESFIRMA AC AAPP*
Name	*[es]*	*Certificados Reconocidos emitidos por ESFIRMA AC AAPP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6494265473925466579*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIKDCCBhCgAwIBAgIIWiBEClppSdMwDQYJKoZIhvcNAQENBQAwgdMxGDAWBgNVBGEMD1ZBVEVT
LUE1MDg3ODg0MjEYMBYGA1UEAwwPRVNGSVJNQSBBQyBSQUlaMSwwKQYDVQQLDCJBVVRPUkIEQUQg
REUgQ0VSVEIgSUNBQ0lPTiBFU0ZJUk1BMRYwFAYDVQQKDA1BVUxPQ0UgUy5BLlUuMUswSQYDVQQH
DEJaYXJhZ296YSAoc2VlIGN1cnJlbnQgYWRkcmVzcyBhdCBodHRwczovL3d3dy5lc2Zpcm1hLmNv
bS9kb2MtcGtpLykxCzAJBgNVBAYTAkVTMB4XDTE2MDQyODE2MDUxNFoXDT15MDQyODE2MDUxNFow
gdoxGDAWBgNVBGEMD1ZBVEVTLUE1MDg3ODg0MjEYMBYGA1UEAwwPRVNGSVJNQSBBQyBBQVBQMTIw
MAYDVQQLDCIBVVRPUkIEQUQgREUgQ0VSVEIgSUNBQ0lPTiBFU0ZJUk1BIC0gQUFQUDEWMBQGA1UE
CgwNQVVMT0NF1FMuQS5VLjFLMEkGA1UEBwxCWmFyYWdvemEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgaHR0cHM6Ly93d3cuZXNmaXJtYS5jb20vZG9jLXBraSSpMQswCQYDVQQGEwJFUzCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAJybLPMHyZ6e7SBmK4S8sCHeeDtZGibPtjPGdEnCESnFG
GLwI23YO+PHn9Cbo5x2eWkXRLvKxt8LZrc5/wGXmAGnD2FD/hJauE4jbC08joe6VXIPkTMEn3GVa
vsJCkhxiM58FBY/cZIdB1AdAU7yaWFlouUDH+uj8O3d2cisN2QqgnIjdcCMHVPbLyOsyTzkOV7oz
8Ujo5d/XVY+GcEsmab8yFcMoTqdwSgXld6xrMWqt5QKWA4lLQK9yTlUOYB45tUvr+QdHpb48M2lK
vexvQFCul3vrk/yrRdLLAnmWttEBZEcwRui9dMipteeRV3YaaX4OiJvo8v764X5pyOEcPZDUeH
OacAguHinqTIfNI3V6dozdCNtUmXL+IPWCdsrx3abGGB4ZPE4gkKt0hFij/VdlIfIvYmOzWlkUHw8
2hoLIJXdrJm/AxGx88qiPvWvGEBmx21aQsDP05tFu3ZZqAlcvZVfLpd1HELCfP0hWHArN37N8JjB
4bNQG1ui+9+sI2WID2EjMtRuiM2k2YZCSIldU54L WOqTK1DOJWOqMMtK4vUvOdwgp6qxU7rCeKau
OLk/RR+nbnbAk6O3unvTuYujmZTB+u0H1n40OBNVFE5GwMT+NZ4GpkKMERtbLjCiPUi/1masde
+RwWosEQtKpNvYknTs4BiDHUgbVR8bzAgMBAAGjggH1MIIB8TBOBggrBgEFBQcBAQRCME AwPgY1
KwYBBQUHMAKGMmh0dHBzOi8vd3d3LmVzZmlybWEuY29tL2RvYy1wa2kvZXNmaXJtYS1hY3JhaXou
Y3J0MB0GA1UdDgQWBBRhiWy7PB69LUTgy/BnQCmATbWjUDASBgNVHRMBAf8ECDAGAQH/AgEAMB8G
A1UdIwQYMBaAFPzvsx7leDX3Kzk/FrT1jMHRcbKZMIGsBgNVHSAEgaQwgaEwgZ4GBFUdIAAwgZUw
LAYIKwYBBQUHAgEWIGh0dHBzOi8vd3d3LmVzZmlybWEuY29tL2RvYy1wa2kvMGUGCCsGAQUFBwIC
MFkMV0F1dG9yaWRhZCBkZSBjZXJ0aWZpY2FjacOzbiBJbnRlcm1lZGlhIGRlIGVzRmlybWEuIFZl
ciBodHRwczovL3d3dy5lc2Zpcm1hLmNvbS9kb2MtcGtpLzBvBgNVHR8EaDBmMDGgL6AthitodHRw
czovL2NybHMxLmVzZmlybWEuY29tL2FjcmFpei9hY3JhaXouY3JsMDGgL6AthitodHRwczovL2Ny
bHMyLmVzZmlybWEuY29tL2FjcmFpei9hY3JhaXouY3JsMA4GA1UdDwEB/wQEAwIBBjAbBgNVHREE
FDASgRBpbmZvQGVzZmlybWEuY29tMA0GCSqGSIb3DQEBDQUAA4ICAQBPpVC113eQwunnwRyTaYIw
A5oWtbdANs0blzlrt52/V384DzdY1WQRHIJwrLcy7KRzdVSC1loCVdoRneINCjv0dVaaJOHy11SD
oSoSsQ1UopES1Ck3nQ+xV0UTKI1uRhFzA6cx53hyeaJCQcUnzIqhpPhOB5HoNmrioFhd00IXIp1e
EvETKwOKNArvCnYdAY8oNnKTFX13w/X6dmIjfbV8yZ02kus1znNHpjqBGAvfG3+PfPkqv8QZet6c
3VOV7ZYL6FtgUoOj/9ac7IIPbEPSUGlbh30Ye8M26vSiMNUQ1FOXLXBDq52maXA84a+jquN0fu4
xOYvBMmxh+GcK+2jkzW7ujidzGi6Tr4al1k04rhA2bOl/Y4ZAfQ8l11TXtfloKSbFZWeHVoz1naN
ExwTKZH7Rqw7jrC1jB86eRd57q5cFtKTrGtdg0tT96NvsPQsGdfbXv+f7Dux6xnm+V8xaQ6X0Ndm
ioI6b5yoBfp8bUellAYfdGQmPYdVQTt5rbRU3dQtUX2eZQRG0m+LdkMGhmB0dlVHjmDY+yBPxc
Ln2wfL6L4nz112vaEyLaMyTg3q7y51bo7dnctfEwe4cA5mYTmG3rArAP+MnIQTtKhpG+yY4Avp/7T
CQJsRS8HMY8kOXaRk5AVnStfm3q9zxNfyGjmd776bzuEwSI6VbOctg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer L:	*Zaragoza (see current address at https://www.esfirma.com/doc-pki/)*
Issuer O:	*AULOCE S.A.U.*
Issuer OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA*
Issuer CN:	*ESFIRMA AC RAIZ*
Issuer 2.5.4.97:	*VATES-A50878842*
Subject C:	*ES*
Subject L:	*Zaragoza (see current address at https://www.esfirma.com/doc-pki/)*
Subject O:	*AULOCE S.A.U.*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*
Subject CN:	*ESFIRMA AC AAPP*
Subject 2.5.4.97:	*VATES-A50878842*
Valid from:	*Thu Apr 28 18:05:14 CEST 2016*
Valid to:	*Sat Apr 28 18:05:14 CEST 2029*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:9B:2C:F3:07:C9:9E:9E:ED:20:66:2B:84:BC:B0:21:DE:78:37:76:19:B3:ED:8C:F1:9D:12:70:84:4A:71:46:18:BC:09:DB:76:0E:F8:F1:E7:F4:2A:E1:A3:9C:76:CD:69:17:F0:BB:CA:C6:DF:0B:67:3B:F9:FF:01:97:98:01:A7:0F:61:43:FE:12:5A:B8:4E:23:6C:EF:23:A3:A5:57:94:F9:08:4C:C1:27:DC:65:5A:BE:C2:42:92:1C:62:33:9F:05:05:8F:DC:64:87:41:D4:07:40:53:BC:9A:58:59:68:B9:40:C7:FA:E8:FC:3B:77:76:72:2B:0D:D9:0A:A0:9C:88:DD:70:23:07:54:F6:CB:C8:EB:32:4F:39:0E:57:BA:33:F1:48:E8:E5:DF:D7:55:8F:86:70:4B:26:69:BF:32:15:C3:28:4E:A7:70:4A:05:E5:77:AC:6B:31:6A:AD:E5:02:96:03:89:4B:40:AF:72:4E:55:0E:60:1E:39:B5:4B:EB:F9:07:47:A6:1E:3C:33:69:4A:BD:EC:6F:40:50:AE:97:7B:EB:93:FC:AB:45:D2:CB:02:79:96:B6:D1:01:64:47:30:45:A8:BD:74:C8:A9:B5:C7:91:57:76:1A:69:F5:F8:3A:22:6F:A3:CB:FB:EB:85:F9:A7:24:04:0A:B3:D9:0D:47:87:39:A7:00:82:ED:47:8A:7A:93:21:F3:48:DD:5E:9D:A3:37:42:36:25:26:5C:BF:88:3D:60:9D:B3:3B:F7:6A:11:86:07:86:4F:13:88:24:2A:DD:21:16:D8:FF:55:D9:47:6D:89:90:CD:62:64:50:7C:3C:DA:1A:0B:20:95:DD:AC:99:BF:03:11:B1:F3:CA:A2:3E:F5:AF:18:40:66:C7:6D:5A:42:C0:CF:D3:9B:45:BB:76:59:A8:09:5C:BD:95:5F:2E:97:75:1C:42:C2:7C:FD:21:58:70:2B:37:7E:CD:F0:98:C1:E1:B3:50:1B:5B:A2:FB:DF:AC:27:65:88:0F:61:23:32:D4:6E:88:CD:A4:D9:86:42:49:F2:1D:53:9E:0B:58:EA:93:28:80:CE:25:63:AA:30:CB:4A:E2:F5:2F:39:DC:20:A7:AA:B1:53:BA:C2:78:A6:AE:38:B9:3F:45:1F:A7:6E:76:C0:93:A3:B7:BA:7B:D3:B9:8B:A3:99:94:C1:FA:E9:74:1F:59:F8:D0:E0:4D:54:51:39:1B:03:13:F8:D6:78:1A:99:0A:30:44:6D:6C:B8:C2:88:F5:3F:8B:FD:66:6A:C7:5E:F9:1F:F0:5A:8B:04:41:F2:A9:36:F6:24:9D:37:B8:06:20:C7:52:06:D5:47:C6:F3:02:03:01:00:01*
Authority Info Access	*https://www.esfirma.com/doc-pki/esfirma-acraiz.crt*
Subject Key Identifier	*61:89:6C:BB:3C:1E:BD:2D:44:E0:CB:F0:67:40:29:80:4D:B5:A3:50*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*FC:EF:B3:1E:C8:78:35:F7:2B:39:3F:16:D4:F5:8C:C1:D1:71:B2:99*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.esfirma.com/doc-pki/* *CPS text: [Autoridad de certificación Intermedia de esFirma. Ver https://www.esfirma.com/doc-pki/]*
CRL Distribution Points	*https://crls1.esfirma.com/acraiz/acraiz.crl* *https://crls2.esfirma.com/acraiz/acraiz.crl*
Subject Alternative Name	*info@esfirma.com*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *A2:8B:23:0D:EF:38:3D:C6:A0:39:5F:37:63:E1:01:CC:8C:3F:F6:4D:96:2C:6A:F3:3A:59:28:41:A9:61:26:82*

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza (see current address at https://www.esfirma.com/doc-pki/)*

Subject O: *AULOCE S.A.U.*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Subject CN: *ESFIRMA AC AAPP*

Subject 2.5.4.97: *VATES-A50878842*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2018-06-25T00:00:00Z

Scheme Service Definition URI

URI *[en]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

28.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47281.1.2.1*

28.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

28.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

28.1.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

28.1.5 - History instance n.1 - Status: granted

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service Name		
Name	*[en]*	*Qualified Certificates issued by ESFIRMA AC AAPP*
Name	*[es]*	*Certificados Reconocidos emitidos por ESFIRMA AC AAPP*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza (see current address at https://www.esfirma.com/doc-pki/)*
Subject O:	*AULOCE S.A.U.*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*
Subject CN:	*ESFIRMA AC AAPP*
Subject 2.5.4.97:	*VATES-A50878842*

X509SKI

X509 SK I	*YYlsuzwevS1E4MvwZ0ApgE21o1A=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2018-05-24T00:00:00Z*

28.1.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47281.1.2.1*

28.1.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

28.1.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

28.1.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

28.1.6 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ESFIRMA AC AAPP*
Name	*[es]*	*Certificados Reconocidos emitidos por ESFIRMA AC AAPP*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza (see current address at https://www.esfirma.com/doc-pki/)*

Subject O:	*AULOCE S.A.U.*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*
Subject CN:	*ESFIRMA AC AAPP*
Subject 2.5.4.97:	*VATES-A50878842*

X509SKI

X509 SK I	*YYlsuzwevS1E4MvwZ0ApgE21o1A=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

28.1.6.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	*[en]*	*undefined.*
	[es]	*undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47281.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47281.1.2.2*

28.1.6.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

28.1.7 - History instance n.3 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ESFIRMA AC AAPP*
Name	*[es]*	*Certificados Reconocidos emitidos por ESFIRMA AC AAPP*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject L:	*Zaragoza (see current address at https://www.esfirma.com/doc-pki/)*
Subject O:	*AULOCE S.A.U.*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*
Subject CN:	*ESFIRMA AC AAPP*
Subject 2.5.4.97:	*VATES-A50878842*

X509SKI

X509 SK I	*YYlsuzwevS1E4MvwZ0ApgE21o1A=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2016-06-23T22:00:00Z*

28.1.7.7 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*
	[es]	*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47281.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47281.1.2.2*

28.2 - Service (withdrawn): Qualified timestamps issued by ESFIRMA TSA

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by ESFIRMA TSA*

Name *[es]* *Sellos de tiempo cualificados emitidos por ESFIRMA TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *341928503678414525*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJKzCCBxOgAwIBAgIIBL7GKZbVLr0wDQYJKoZIhvcNAQELBQAwgdoxGDAWBgNVBGEMD1ZBVEVT
LUE1MDg3ODg0MjEYMBYGA1UEAwwPRVNGSVJNQSBBQyBBQVBQMTIwMAYDVQQLDCIBVVRPUklEQUQg
REUgQ0VSVEIGSUNBQ0lPTiBFU0ZJUk1BIC0gQUFQUDEWMBQGA1UECgwNQVVMT0NFIFMuQS5VLjFL
MEkGA1UEBwxCWmFyYWdvemEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgaHR0cHM6Ly93d3cuZXNm
aXJtYS5jb20vZG9jLXBraS8pMQswCQYDVQQGEwJFUzAeFw0xNzA1MjMxMzI4MDVaFw0yNTA1MjMx
MzI4MDVaMIGVMQswCQYJVQQGEwJFUzERMA8GA1UEBwwIWmFyYWdvemExFjAUBgNVBAoMDUFVTE9D
RSBTLkEuVS4xKzApBgNVBAsMIkFVVE9SSURRBCBERSBDRVJUSUZJQ0FDSU9OIEVTRklSTUEsGDAW
BgNVBGEMD1ZBVEVTLUE1MDg3ODg0MjEUMBIGA1UEAwwLRVNGSVJNQSBUU0EwggIiMA0GCSqGSIb3
DQEBAQUAA4ICDwAwggIKAoICAQCRYKk/rgPI+StcuWHbGPrN92Xo8UuUR0L1mIsLrEHBFb0s0fIy
3GoK9fIXH1+mUlN7IqAjswKX3QMNorhtu7IV+IOb+SFK1BI+d9877K0xDumolrAIUKHj94gcuZwu
6fpLEKSR02gKfqULwbsbG6dIrBFuGNtbC90BCMQnX9q7SYjjz2alxeRSQmLOfunT8Kubt07cSFpr
s5Vs427weJuthJbRtD2q028LTHST9R8klV7dRqoHhic6x/+48DLPgxUeGI0jt+lixnLuAUlszkTm
KcAG8GvMPG2J2z7j6xQP4vjA9kxQ4jhlV0JOC8DyuNtiMczwecgJDCdDQ0YVvgk2fvvf/hs2cI+8
gv+YZQN9ex5m9mE50Ry+0ddWWuRp9vB273WvbdjGvwDy49bmkcNeRuYVAIk6u3CXcmoEYZqjNmBR
k9k8FccPCnsUNZJVyYI65LTTKz3UDWSdZTmEYcDyeT5MKVV+UG1+2hI9gxwoM4TFeNLn6ZvTIw3g
1xWFr8tkMesRkD6G1DkEC1sUyKi55EKrG/L3Cn9I4uI1tMRW++jcEBet633EU3GiUc9cnRDWr2I9f
saqi6B4VhEYbZaByqcux5HIOvzybv4VnM0ltzp/OPLN4566TFHArVdP2KcshvIT+aBpraHNJosV
E6VZUETr4+7AIW9yUn20ptxctwIDAQABo4IDNjCCAzIwgboGA1UdIASBsjCBrzAJBgcEAIvsQAEB
MIGibBgsrBgEEAYLxMQEFAQCBkTAsBggrBgEFBQcCARYgaHR0cHM6Ly93d3cuZXNmaXhYS5jb20v
ZG9jLXBraS8wYQYIKwYBBQUHAgIwVQx7U2Vydmlkb3IgZGUgc2VsbGFkbyBkZSB0aWVtcG8gZGUg
ZXNGSVJNQS4gQ29uc3VsdGUgaHR0cHM6Ly93d3cuZXNmaXhYS5jb20vZG9jLXBraS8wHQYDVR0O
BBYEFDRq0hURMt0c3adZj+k1Jl6m/I53MB8GA1UdIwQYMBaAFGGJbLs8Hr0RODL8GdAKYBNlaNQ
MA4GA1UdEwQCMAAwDgYDVR0PAQH/BAQDAgZAMBYGA1UdIQEB/wQMMAoGCCsGAQUFBwMIMG0GA1Ud
HwRmMGQwMKAuoCyGKmh0dHA6Ly9jcmxzMS5lc2Zpcm1hLmNvbS9hY2FhcHAvYWNhYXBwLmNybDAw
oC6gLIYqaHR0cDovL2NybHMyLmVzZmlybWEuY29tL2FjYWFwcC9hY2FhcHAuY3JsMIGrBggrBgEF
BQcBAQSBnjCBmzAsBggrBgEFBQcwAYYgaHR0cDovL29jc3AxLmVzZmlybWEuY29tL2FjYWFwcC8w
LAYIKwYBBQUHMAGGIGhkdHA6Ly9vY3Nwb3Sc2Zpcm1hLmNvbS9hY2FhcHAvMDQ6CCsGAQUFBzAC
hjFodHRwOi8vd3d3LmVzZmlybWEuY29tL2RvYy1wa2kvZXNmaXJtYS1hY2FhcHAuY3J0MIHFBggr
BgEFBQcBAwSBuDCBtTAIBgYEAI5GAQEwEwYGBACORgEGMAkGBwQAjkYBBgIwCwYGBACORgEDAgEP
MHAGBgQAjkYBBTBmMDEWK2hldHBzOi8vd3d3LmVzZmlybWEuY29tL2RvYy1wa2kvUERTL1RTMi1F
TiBTAmVuMDEWK2hldHBzOi8vd3d3LmVzZmlybWEuY29tL2RvYy1wa2kvUERTL1RTMi1FUy8TAmVz
MBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwGwYDVR0SBBQwEoEQaW5mb0Blc2Zpcm1hLmNvbTANBgkq
hkiG9w0BAQsFAAOCAgEAO7S+ozE+QhZLpFTVjJdjdlMqY+5kSqYtjTW+r77La4JCKHNlJ9T49Tbi
+SmNJQ7gC/OTKzha6DMOMzANqg2zahhJisVyf14hF0Sfh2ncA9jmKztFcMIA/i6/h1y+JdK/XM/k
Kgt64uYop7UcgiksrBiPAcDcijkaiwIig0dXsYfrYEYYj+DJgMtAKMMTEH/luhMxbZycZJsLLxtNu
68yLjSvMfiqJekx2zU/fcldK2nd0yu2oqr+zgmsaifmIHLplenkCqh2TFp7ce5zIHRysbPObPFts2
tXNdUZV8DQkbKOtfDZ5x7mniLwYnP4AT52oOn7HvNR4OszzUmVsS/mn3GWDGDnaYoqfviow+0Fst
EpjqzmOAz7Gofl2vx6+8UR5a5YKpDG6klMzNB+PdPcxLvX4DRYnHPIcgHn3CAQtao8pobKZukQSb
90Eh098qpmOtaWR3Io1r5+1wgMbPVsz1NHCFXY+tDNI3dIxpoRunDU44jvIz1nRBZsPPtK9whUz63
+VDGbb3WzKCK9uuIW9F/zWNcxsR21rD7IZmEryvd86WUjq0pIL9zOYAXobmI0E2ogz+Wsd7U/vU2
lml6Us9PQT9b1AFdyYyQmxAnhP7N16bzC2aW221CWnrUKR/InsP5CN+9lBDWDnu3qnmq1/MsXUwE
7ezcWWGm/Vcg2piDUkE=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L: *Zaragoza (see current address at https://www.esfirma.com/doc-pki/)*

Issuer O: *AULOCE S.A.U.*

Issuer OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Issuer CN: *ESFIRMA AC AAPP*

Issuer 2.5.4.97: *VATES-A50878842*

Subject CN: *ESFIRMA TSA*

Subject 2.5.4.97: *VATES-A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA*

Subject O: *AULOCE S.A.U.*

Subject L: *Zaragoza*

Subject C: *ES*

Valid from: *Tue May 23 15:28:05 CEST 2017*

Valid to: *Fri May 23 15:28:05 CEST 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:60:A9:3F:AE:03:C8:F9:27:DC:B9:61:DB:18:FA:CD:F5:95:E8:F1:4B:94:47:42:E6:22:C2:EB:10:70:45:87:4B:34:7E:D2:72:DC:6A:0A:F4:79:57:1F:5F:A6:52:53:7B:96:A0:23:B3:02:97:DD:03:0D:A2:B8:6D:BB:B2:55:F8:83:A1:F9:21:4A:D4:12:3E:77:DF:3B:EC:AD:31:0E:E9:E8:96:B0:25:50:A1:E3:F7:88:1C:B9:9C:2E:E9:FA:4B:10:A4:91:D3:68:0A:7E:A5:0B:C1:BB:1B:1B:A7:48:AC:11:6E:18:DB:61:0B:DD:01:08:C4:27:5F:DA:93:E5:88:E3:CF:66:A5:C5:E4:52:42:62:CE:7E:E9:D3:F0:AB:9B:8B:4E:DC:48:5A:6B:B3:95:6C:E3:6E:F0:78:9B:AD:6C:96:D1:B4:3D:AA:D3:6F:0B:4C:74:93:F5:1F:24:95:5E:DD:46:AA:07:86:27:3A:C7:FF:B8:F0:32:CF:83:15:1E:1A:5D:23:B7:E9:62:C6:72:EE:01:49:6C:CE:44:E6:29:E0:06:F0:6B:CC:3C:6D:99:DB:3E:E3:EB:14:0F:E2:F8:C0:F6:4C:50:E2:38:65:57:42:4E:0B:C0:F2:B8:DB:62:31:CC:F0:79:C8:09:0C:27:43:43:46:15:BE:09:36:7E:FB:DF:FE:1B:36:70:8F:BC:82:FF:98:65:03:7D:7B:1E:66:F6:61:39:D1:1C:BE:D1:D7:56:5A:E4:69:F6:F0:76:EF:75:AF:6D:D8:C6:BF:00:F2:E3:D6:E6:91:E3:5E:46:E6:15:00:89:3A:BB:70:97:72:6A:04:61:9A:A3:36:60:51:93:D9:3C:15:C7:0F:0A:7B:14:35:98:D5:C9:89:7A:E4:B7:D3:2B:3D:D4:0D:64:AD:65:39:84:61:C0:F2:79:3B:0C:29:55:7E:50:6D:7E:DA:12:3D:83:1C:28:33:84:C5:78:D2:E7:E9:9B:D3:97:02:60:D7:15:85:AF:CB:64:31:EB:11:90:3E:86:D4:39:04:0B:5B:14:C8:A8:B9:10:AA:C6:FC:BD:C2:9F:D2:38:B9:FD:6D:31:15:BE:FA:37:04:05:EB:7A:DF:71:14:DC:68:94:73:D7:27:44:35:AB:D9:FF:5F:B1:AA:A3:E8:1E:15:84:46:1B:65:A0:72:A9:CB:B1:E4:72:0E:BF:3C:9B:BF:85:67:33:42:2D:CE:9F:CE:3C:B3:78:E7:AE:93:14:70:22:AD:57:4F:D8:A7:AC:86:F9:53:F9:A0:69:AD:A1:CD:26:8B:15:13:A5:59:50:44:EB:E3:EE:C0:95:6F:72:52:7D:B4:A6:DB:31:B7:02:03:01:00:01

Certificate Policies

Policy OID: 0.4.0.194112.1.1

Policy OID: 1.3.6.1.4.1.47281.1.5.2

CPS pointer: https://www.esfirma.com/doc-pki/

CPS text: [Servidor de sellado de tiempo de esFIRMA. Consulte https://www.esfirma.com/doc-pki/]

Subject Key Identifier *34:6A:D2:15:11:32:DD:1C:DD:A7:59:8F:E9:09:D4:8E:A6:FC:8E:77*

Authority Key Identifier *61:89:6C:BB:3C:1E:BD:2D:44:E0:CB:F0:67:40:29:80:4D:B5:A3:50*

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points

http://crls1.esfirma.com/acaapp/acaapp.crl

http://crls2.esfirma.com/acaapp/acaapp.crl

Authority Info Access

http://ocsp1.esfirma.com/acaapp/

http://ocsp2.esfirma.com/acaapp/

http://www.esfirma.com/doc-pki/esfirma-acaapp.crt

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

Issuer Alternative Name *info@esfirma.com*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A7:DC:18:B2:E8:2F:38:19:8E:AC:20:69:90:EE:5C:62:B9:85:92:82:A5:AB:B7:7A:C2:A8:65:A5:85:2C:97:A2*

X509SubjectName

Subject CN: *ESFIRMA TSA*

Subject 2.5.4.97: *VATES-A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA*

Subject O:	*AULOCE S.A.U.*
Subject L:	*Zaragoza*
Subject C:	*ES*

X509SKI

X509 SK I	*NGrSFREy3Rzdp1mP6QnUjqb8jnc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2018-06-25T00:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

28.2.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name	*[en]*	*Qualified timestamps issued by ESFIRMA TSA*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por ESFIRMA TSA*

Service digital identities

X509SubjectName

Subject CN:	*ESFIRMA TSA*
Subject 2.5.4.97:	*VATES-A50878842*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA*
Subject O:	*AULOCE S.A.U.*
Subject L:	*Zaragoza*
Subject C:	*ES*

X509SKI

X509 SK I	*NGrSFREy3Rzdp1mP6QnUjqb8jnc=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2018-05-24T00:00:00Z*

28.3 - Service (granted): Qualified Certificates issued by ESFIRMA AC AAPP 2

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by ESFIRMA AC AAPP 2*
Name	*[es]*	*Certificados Cualificados emitidos por ESFIRMA AC AAPP 2*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*4761709294065530426*
X509 Certificate	


```
-----BEGIN CERTIFICATE-----
MIIHiDCCBeSgAwIBAgIIQhT9X9RztjowDQYJKoZIhvcNAQENBQAwgbUxCzAJBgNVBAYTAkVTMREw
DwYDVQQHEwhaQVJBR09aQTE2MDQGA1UEChMtRVNQVUJMSUNPIFNFUiZJQ0lPUyBQQVJBIExBIEFE
TUlOSVNUUkFDSU9OIFNBMSswKQYDVQQLEyJBVVRPUkIEQUQgREUgQ0VSVEIGSUNBQ0lPTiBFU0ZJ
Uk1BMRIwEAYDVQQFEwlBNTA4Nzg4NDIxGjAYBgNVBAMTEUVTRkISTUEgQUMgUkFJWiAyMB4XDTE3
MTEwMjEzMTI0N1oXDTMwMTEwMjEzMTI0N1owgbwxC2AJBgNVBAYTAkVTMREwDwYDVQQHEwhaQVJB
R09aQTE2MDQGA1UEChMtRVNQVUJMSUNPIFNFUiZJQ0lPUyBQQVJBIExBIEFETUlOSVNUUkFDSU9O
IFNBMTIwMAYDVQQLEyIBVVRPUkIEQUQgREUgQ0VSVEIGSUNBQ0lPTiBFU0ZJUk1BIC0gQUFQUDES
MBAGA1UEBRMJQTUwODc4ODQyMRowGAYDVQQDExFUU0ZJUk1BIEFDIEFBUFAgMjCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAIwpCKSodYWYDxHDVl+jR0c50Hf0WxU/+t6i3x1biQ9wRwMLBP
IWAJyCKOkYnjcucpA5YqPmCS98JbS+cRM6zDC9PA1Pb V1csxWha2Om3Y1kUUPSxVTfycKIRsW7Q
ClNtvtXx6gDcfcVsAYI6fskQ9iP9LCN8BTfxDwJaDRtEf9ENi6OxyMW4pDPlp026aht4K7o7t1pr
DisuY9qcfit2t//DNn03z/ZOTtr/c8TywSPuaanLdk6OqWfA8QNFBgM8ocOArlnmj6c8cwJ46fBl
s4I4e7BvZmoS2EQ62n9H0kJ/CVFyQh6ydD8dqgLzRozjDjXYMANMrIL17mEUCOUUHaHBjXxPCNz
DTlcQ66jKV8xGWdyZKkrCCEuX5OP77yr6TgdEvThxwvtpuToeHSACy+Vb6c6PRmaAwb7J5qPqq4F
SpcWCRGm2xbMQuwYiEHBcqIMSrDWyGoP4Fq2FlzPQcz37gotv8+nGJMmgIR6v6jWXVjvSy+SdzkK
aNQrspMk2IG9ouz6SS/77V2ghzrmWMfWH8S/c0mrmxsFZ9p3lPDrCgOyp7eYX7vFzGUbQqhUrpow
rZUUtzNk4RgMi+Q22kbkJtTYXML9C8DIDd5ZaaaZ49FVwIzzDBbX/Czlhs87w8YZw+iVlcpKyNt+
nUzy1JHHSyFmlOhu3cZevWAhLyOdAgMBAAGjggIFMIICATB9BggrBgEFBQcBAQRxMG8wPwYIKwYB
BQUHMAKGM2h0dHBzOi8vd3d3LmVzZmlybWEuY29tL2RvYy1wa2kvZXNmaXJtYS1hY3JhaXoyLmNy
dDAsBggrBgEFBQcwAYYgaHR0cDovL29jc3AuZXNmaXJtYS5jb20vYWNyYWl6Mi8wHQYDVR0OBBYE
FPZA78Onk03IvzHp+u7DcXkfKgNYMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUg4DI
1ie97zCyrh2dyqjyMhTHEzIwggqGA1UdIASBoDCBnTCBmgYEVR0gADCBkTAsBggrBgEFBQcCARYg
aHR0cHM6Ly93d3cuZXNmaXJtYS5jb20vZG9jLXBraS8wYQYIKwYBBQUHAgIwVQxTQXV0b3JpZGFk
IGRlIGNlcnRpZmlj YWNpw7NuIEFBUFAgMiBkZSBlc0ZpcmlhLiBWZXlgaHR0cHM6Ly93d3cuZXNm
aXJtYS5jb20vZG9jLXBraS8wcQYDVR0fBGowaDAyoDCgLoYsaHR0cHM6Ly9pcmxzNS5lc2ZpcmIh
LmNvb5ybY3JhaXovYWNyYWI6Mzcmwwq4wwC6GLGhb0HBzOi8vd3d3cuZXNmaXJtYS5jb20v
YWNyYWI6L2FjcmFpejIuY3JsMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQ0FAAOCAgEAgGo1
ZvgB5neEOob/p5MQOtcdUtjZVGVyLKO63n116SvkGFfU/M/Z1HkKVQ0ecwBDT1iP7GgEU2REOoa
zb5ExGUV4opQgz1Ywt5cK9xgv3STj31gCPt+kX8R4trxOwYFWK64AbCHxtEXlCPZQN91w6d8+n9Nb
nsmnzuvO4QQAscMZeW/7Ti+fdgvEiZW/IFsYPsK2U7N3/jiNaWiTHKPndIQZcs9Gb+Mc8u0VIZT
QbpwNAFv1E+qrRhDseuW3FfSVMl6V9/0DAdQTC2awGK/VxWbLEfjCD5kbIC7oWTkzYLuK/C/vCH1
YxQ+Tg185vz5RNbNSJSnlKNlibwtSwUbs9eBuEAiv14ZND2h02gotZjJ5sZY62qKbYVms17nH/WS
8lMBShuZeUC2ona9ebMGk/9YMBrvJjnj9uzT1art3qH0AIH2F0m4VgQTlt3kM6u1otn8sx4dJ5g/
4mBtF9vRNuoYbXAv6tGryWzdCkMqh716ZOffiNipqqTA9/RPXSzf1aBgsyrUE45IFnb9VSYMb+nA
zLSZjUECxH2DlodM4QKxUtQz0W0B4Qyoh/ccbT2jpRNXt8OQE3vnnCaHR3qag5KmMD1hjI1T83v6
jWF2f0ckDknnrwE/FmwSFClatQiKuiacDqyyJjhM25sBthb+xq2wwu7yIY22MSJlR8TkOc=

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA512withRSA*
Issuer CN:	*ESFIRMA AC RAIZ 2*
Issuer SERIAL NUMBER:	*A50878842*
Issuer OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA*

Issuer O:	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*
Issuer L:	*ZARAGOZA*
Issuer C:	*ES*
Subject CN:	*ESFIRMA AC AAPP 2*
Subject SERIAL NUMBER:	*A50878842*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*
Subject O:	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*
Subject L:	*ZARAGOZA*
Subject C:	*ES*
Valid from:	*Thu Nov 02 14:12:47 CET 2017*
Valid to:	*Sat Nov 02 14:12:47 CET 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:88:B0:A4:22:B9:A1:D6:16:21:7B:07:0D:52:3E:8D:18:79:D0:7D:16:C5:4F:A2:EA:2D:F1:D6:18:90:F7:04:70:30:B0:4F:95:60:09:C8:22:8E:91:89:E3:72:E7:29:03:96:2A:3E:60:92:F7:C2:5B:4B:E7:11:33:AC:C3:0B:D3:C0:D4:F6:D5:D5:CB:31:5A:16:B6:3A:6D:D8:D6:45:14:3D:2C:55:4D:FC:9C:28:87:CA:B1:6E:D0:0A:53:6D:BE:D5:F1:EA:00:DC:7D:E5:6C:01:82:3A:7E:C9:10:F6:23:FD:2C:23:7C:05:37:F1:0F:02:5A:0D:FB:44:7E:D1:0D:8B:A3:B1:C8:C5:B8:A4:33:E5:A7:4D:BA:6A:1B:78:2B:BA:3B:B7:5A:6B:0E:2B:2E:63:DA:9E:7E:2B:76:B7:FF:C3:36:7D:37:CF:F6:4E:4E:DA:FF:73:C4:F2:C1:23:EE:69:A9:CB:76:4E:8E:A9:67:C0:F1:03:45:06:03:3C:A1:C3:80:AE:59:E6:8F:A7:3C:73:02:78:E9:F0:65:B3:82:38:7B:B0:6F:66:6A:12:D8:44:3A:DA:7F:47:D2:42:7F:09:51:72:42:1E:B2:74:30:5D:AA:A2:EB:46:8C:E3:0E:35:D8:30:03:4C:AE:52:CB:23:B9:84:50:23:94:50:76:87:06:35:F1:3C:23:73:0D:32:1C:43:AE:A3:29:5F:31:19:67:72:64:A9:2B:08:21:2E:5F:93:8F:EF:BC:AB:E9:38:1D:12:F4:E1:C7:0B:ED:A6:E4:E8:70:74:80:0B:2F:95:6F:A7:3A:3D:19:9A:03:06:FB:27:9A:8F:AA:AE:05:4A:97:96:09:11:A6:DB:16:CC:42:EC:18:88:41:C1:72:A2:0C:4A:B0:D6:C8:6A:0F:E0:5A:B6:16:5C:CF:41:EC:F7:EE:0A:2D:BF:CF:A7:18:93:26:81:F4:7A:BF:A8:D6:5D:58:EF:4B:2F:92:77:39:0A:68:D4:2B:B2:93:24:D8:81:BD:A2:EC:FA:49:2F:FB:ED:5D:A0:87:3A:E6:58:C7:D6:1F:CE:7F:73:49:AB:9F:1B:05:67:DA:77:94:F0:EB:1A:03:B2:A7:B7:98:5F:BB:C5:CC:65:1B:42:A8:54:AE:9A:30:AD:95:14:AE:D3:64:E1:18:0C:8B:E4:36:DA:48:4A:95:F4:D8:5C:C2:FD:0B:C0:E5:0D:DE:59:91:A6:99:E3:D1:55:C0:8C:F3:0C:18:57:FC:2C:E2:86:C4:7B:C3:C6:19:C3:E8:95:95:CA:4A:C8:DB:7E:9D:4C:F2:D4:91:C7:4A:F1:66:94:E6:EE:DD:E6:5E:BD:60:21:2F:23:9D:02:03:01:00:01*
Authority Info Access	*https://www.esfirma.com/doc-pki/esfirma-acraiz2.crt* *http://ocsp.esfirma.com/acraiz2/*
Subject Key Identifier	*F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*83:80:E5:D6:27:BD:EF:30:B2:AE:1D:9D:CA:A8:F2:32:14:C7:13:32*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.esfirma.com/doc-pki/* *CPS text: [Autoridad de certificación AAPP 2 de esFirma. Ver https://www.esfirma.com/doc-pki/]*
CRL Distribution Points	*https://crls1.esfirma.com/acraiz/acraiz2.crl* *https://crls2.esfirma.com/acraiz/acraiz2.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*2C:18:23:61:9D:80:73:11:6C:8F:14:8B:D3:85:79:DE:9C:05:39:16:02:DB:CE:B9:65:73:E4:A1:88:E1:32:6E*

X509SubjectName

Subject CN:	*ESFIRMA AC AAPP 2*
Subject SERIAL NUMBER:	*A50878842*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*
Subject O:	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*
Subject L:	*ZARAGOZA*
Subject C:	*ES*

X509SKI

X509 SK I	*9kDvw6crTeW/Men67sN5eR8qA1g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2021-10-26T01:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

28.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

28.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

28.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by ESFIRMA AC AAPP 2*
Name	*[es]*	*Certificados Cualificados emitidos por ESFIRMA AC AAPP 2*

Service digital identities

X509SubjectName

Subject CN:	*ESFIRMA AC AAPP 2*
Subject SERIAL NUMBER:	*A50878842*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*
Subject O:	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*
Subject L:	*ZARAGOZA*
Subject C:	*ES*

X509SKI

X509 SK I	*9kDvw6crTeW/Men67sN5eR8qA1g=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2018-06-25T00:00:00Z*

28.3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

28.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

28.3.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

28.4 - Service (granted): Qualified timestamps issued by ESFIRMA TSA 2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by ESFIRMA TSA 2*

Name *[es]* *Sellos de tiempo cualificados emitidos por ESFIRMA TSA 2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *131173230648161043*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJjCCBwi6gAwIBAgIIAdlFW7jS8xMwDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAkVTMREw
DwYDVQQHEwhaQVJBR09aQTE2MDQGA1UEChMtRVNQVUJMSUNPIFNFUlZJQ0lPUyBQQVJBIExBIEFE
TUlOSVNUUkFDSU9OIFNBMTIwMAYDVQQLEyIBVVRPUklEQUQgREUgQ0VSVEIGSUNBQ0lPTiBFUlZJ
Uk1BIC0gQUFQUDESMBAGA1UEBRMJQTUwODc4ODQyMRowGAYDVQQDExFUL0ZJUk1BIEFDIEFBUFAg
MjAeFw0xODA2MjAwOTI4MzhaFw0yMzA2MjAwOTI4MzhaMIHLMQswCQYDVQQGEwJFUzERMA8GA1UE
BxMIWkFSQUdPWkExNjA0BgNVBAoTLUVTUFVCTEIDTyBTRVJWSUNJT1MgU1EFSQSBMQSBBRE1JTkIT
VFJBQ0lPTiBTQTEzMCkGA1UECxMiQVVUT1JJREFEIERFIENFUlRJRkIDQUNJT04gRVNGSVJNQTES
MBAGA1UEBRMJQTUwODc4ODQyMRgwFgYDVQRhEw9WQVRFUy1BNTAdNzg4NDIxFjAUBgNVBAMTDUVT
RkISTUEgVFNBIDIwggIiMA0GCSqGSIb3DQEBAQUAAIICDwAwggIKAoICAQCUyFkZLGgagASH5+1i
ZoKDYNFwEbkXdo2RQ5JOo8AuAbOMOd00tbPO+ZF/Xll4vlH75iVyKI2+Xql56EPJrnvgdtUMq5L3
6N0zBQRqo+KpwW6nKU6lgz2XFcB+HQsv/ZUlgKvRw3LMGFqt/QP0TjyzZDjeSplEANppaPmgTtl/
4+s+Dv1krqPsYrx+1DMqkUjT7Sz2MoY46s1MVl6f/VfdR6POJLvX6IBT1FLcREbbT8grsq+Q3WxZ
X6RQvVRUvOnKQhdBbAgZwHRt8DEi1+5kk745Sjwdqcc12587S2KR7B8M3ibHIowFsWUwTpwCMQ2
mx10ukdejKEELei2E2x0OyAZ1NICUQGTqf/mkSmrl7MyPyn3OnvGrk4pJ+Sz970I61y+j2SxQqnX
EbBZ+uD7STP/483jV/+/dmmYnyD/QKtRYM6kyBJ+21xZiJm/g94+kJU94CqELOXELG9tJnNLGwmv
INiT2B1Np4BaBj2hdzuMlEE+cq5BSvVrmPxTW0CxEz6856p1/OGaGyL8x2hKuW+y33My0hCuKdOL
Obp0o+9z9NpxfGzSMG7pTdzk0IIbVyrI1T8o2ybvMuO8vQ/GVCXLR/6597WTzOuXcAC0Bt3umZ5W
0MiKQQg+AnTd2XeZewtkhyvVPzRCV+5+7mF4L8pMfG1ym2Rta4WZ11uigQIDAQABo4IDGTCCAxUw
gboGA1UdIASBsjCBrzAJBgcEAIvsQAEBMIGhBgsrBgEEAYLxMQEFAjCBkTAsBggrBgEFBQcCARYg
aHR0cHM6Ly93d3cuZXNmaXJtYS5jb20vZG9jLXBraS8wYQYJKwYBBQUHAgIwVQxTU2Vydmlkb3Ig
ZGUgc2VsbGFkbyBkZSBlbWVtcG8gZGUgZXNGSVJNQS4gQ2huc3VsdGUgaHR0cHM6Ly93d3cuZXNm
aXJtYS5jb20vZG9jLXBraS8wHQYDVR0OBBYEFC2ml92Hjwfn2D0yH+5p5Dd/VfVdMB8GA1UdIwQY
MBaAFPZA78OnK03lvzHp+u7DeXktKgNYMAkGA1UdEwQCMAAwDgYDVR0PAQH/BAQDAgZAMBYGA1Ud
JQEB/wQMMAoGCCsGAQUFBwMIMG8GA1UdHwRoMGYwMaAvoC2GK2h0dHA6Ly9jcmxzMS5lc2Zpcm1h
LmNvbS9hY2FhcHAvYWNhYXBwMi5jcmwwMaAvoC2GK2h0dHA6Ly9jcmxzMi5lc2Zpcm1hLmNvbS9h
Y2FhcHAvYWNhYXBwMi5jcmwwgacGCCsGAQUFBwEBBIGaMIGXMC0GCCsGAQUFBzABhiFodHRwOi8v
b2NzcDEuZXNmaXJtYS5jb20vYWNhYXBwMi8wLQYIKwYBBQUHMAGGIWh0dHA6Ly9vY3NwMi5lc2Zp
cm1hLmNvbS9hY2FhcHAyLzA3BggrBgEFBQcwAoYraHR0cHM6Ly93d3cuZXNmaXJtYS5jb20vZG9j
LXBraS9hY2FhcHAyLmNydDCBxwYKwYBBQUHAQMEgbowgbcwCAYGBACORgEBMBMGBgQAjkYBBjAJ
BgcEAI5GAQYCMAxGBgQAjkYBAwIBDzByBgYEAI5GAQUwaDAyFixodHRwczovL3d3dy5lc2Zpcm1h
LmNvbS9kb2MtcGtpL1BEUzlvVFMyLUVOLxMCZW4wMhYsaHR0cHM6Ly93d3cuZXNmaXJtYS5jb20v
ZG9jLXBraS9QRFMyL1RTMi1FUy8TAmVzMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwDQYJKoZIhvcN
AQELBQADggIBADStNupoaar+UdJz1B9x4zqgiGZEFrORSPdFdkLowIPZc21o9qWg+nC16CfVO5MY
CKjiNkbcGYNLL8OcXtxYu6CHQG4h5qIamy4k3R3/au7SzXomFr5utiuc5Pb7tK2cfdfl0Y0QgLD
DgJTjC5JgdkwjEZUrQ1cXrHH2ATsvV1apr6wNyGmX7qbLLzZWjntKfX0pC95utsP3kFuQS2wzfZ
V56cXcO/6579KzciSzbYwpJQXfAUvqCyIswKkJtUCEPzAvN4L/eRqb2OZ5MGF1MuDLPK+YEbfgSA
mt4p2aCFQS8QtOv2HozI4YQb9ocKJFZY1OIRX9KLbxIoI+MgtDizXJbuR+t0/218Kiwluxnw MA4Q
fG4e1DbOTR5KCxzuHtAZ4AQ6Z86tMs5NB5elMK+YEIqCTFSRRZO6Ou2ms4SgCKuLxxTZ4m6THU6c
zpEKziKHRqcMkepF4uaIlP8vz9W7EPS/v4HC8u8OiGAXiDd/2TzEATZOXKSkBMk25H4pagLLDJtt
10OD4OtBWrP0d7KlrmoHjwSsvTTalplznbbEF+Dqx5rrN3cjaJn/f87E0gcl8eSw04g5q9Qx+CKZ
cch+1dR/E7/ir6HIi8WdQZMkvQaMxsBKk0evaEQPTQj52umV14wm1gWrwpB7hu1RG/tr+x8w8EJY
l09KCN+ss1jX

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ESFIRMA AC AAPP 2*

Issuer SERIAL NUMBER: *A50878842*

Issuer OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Issuer O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Issuer L: *ZARAGOZA*

Issuer C: *ES*

Subject CN: *ESFIRMA TSA 2*

Subject 2.5.4.97:	*VATES-A50878842*
Subject SERIAL NUMBER:	*A50878842*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA*
Subject O:	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*
Subject L:	*ZARAGOZA*
Subject C:	*ES*
Valid from:	*Wed Jun 20 11:28:38 CEST 2018*
Valid to:	*Tue Jun 20 11:28:38 CEST 2023*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:94:C8:59:19:2C:68:1A:A8:0E:47:E7:ED:62:66:82:83:60:D1:70:11:B9:17:76:8D:91:43:92:4E:A3:C0:2E:01:B3:8C:39:DD:34:B5:B3:CE:F9:91:7F:5E:59:78:BE:51:FB:E6:25:72:2A:5D:BE:5E:A9:79:E8:43:C9:AE:7B:E0:76:D5:0C:AB:92:F7:E8:DD:33:05:04:6A:A3:E2:A9:C1:6E:A7:29:4E:A5:83:3D:97:15:C0:7E:1D:0B:2F:FD:95:08:80:AB:D1:C3:72:CC:18:5A:AD:FD:03:F4:4E:3C:B3:D8:38:DE:4A:92:04:00:DA:69:68:F9:A0:4E:D2:3F:E3:EB:3E:0E:FD:64:AE:A3:EC:62:BC:7E:D4:33:2A:91:48:D3:ED:2C:F6:32:86:38:EA:CD:4C:56:5E:9F:FD:57:DD:47:A3:CE:24:BB:D7:E8:80:53:D4:52:DC:44:46:DB:4F:C8:23:B2:AF:90:DD:6C:59:5F:A4:50:E9:54:54:BC:E9:CA:42:17:41:6C:08:19:C0:74:6B:F0:31:22:D7:EE:64:93:BE:39:4A:28:F0:76:3A:9C:73:5D:B9:F3:B4:B6:29:1E:C1:F0:CD:E2:84:7A:30:16:C5:94:C1:3A:70:08:C4:36:9B:1D:74:BA:47:5E:8C:A1:04:2D:E8:B6:13:6C:74:3B:20:19:D4:D2:02:51:01:93:A9:FF:E6:91:29:AB:97:B3:32:3F:29:F7:3A:7B:C6:AE:4E:29:27:E4:B3:F7:BD:08:EB:5C:BE:8F:64:B1:42:A9:D7:11:B0:59:FA:E0:FB:49:33:FF:E3:CD:E3:57:FF:BF:76:79:98:9F:20:FF:40:AB:51:60:CE:A4:C8:12:7E:DB:5C:59:88:99:BF:83:DE:3E:90:95:3D:E0:2A:84:2C:E5:C4:2C:6F:6D:26:73:4B:1B:09:AF:20:D8:93:D8:1D:4D:A7:80:5A:06:3D:A1:77:3B:8C:94:41:3E:72:AE:41:4A:F5:6B:98:FC:53:5B:40:B1:13:3E:BC:E7:AA:75:FC:E1:9A:1B:22:FC:C7:68:4A:B9:6F:B2:DF:73:32:D2:10:AE:29:D3:8B:39:B8:E9:D2:8F:BD:CF:D3:69:C5:F1:B3:E4:C1:BB:A5:37:73:93:41:DB:57:27:F5:4F:CA:36:C9:BB:CC:B8:E4:AF:43:F1:BF:54:25:CB:47:FE:B9:F7:B5:93:CC:E6:97:C4:00:A5:06:DD:EE:99:9E:56:D0:C8:8A:41:08:3E:02:74:DD:D9:77:99:7B:0B:64:87:2B:D5:3F:34:42:57:EE:7E:EE:61:78:2F:CA:4C:7C:6D:72:9B:64:6D:6B:85:99:D7:5B:A2:81:02:03:01:00:01*
Certificate Policies	*Policy OID: 0.4.0.194112.1.1* *Policy OID: 1.3.6.1.4.1.47281.1.5.2* *CPS pointer: https://www.esfirma.com/doc-pki/* *CPS text: [Servidor de sellado de tiempo de esFIRMA. Consulte https://www.esfirma.com/doc-pki/]*
Subject Key Identifier	*2D:A6:23:DD:87:8F:07:E7:D8:3D:32:1F:EE:69:E4:37:7F:55:F5:5D*
Authority Key Identifier	*F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58*
Basic Constraints	*IsCA: false*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://crls1.esfirma.com/acaapp/acaapp2.crl* *http://crls2.esfirma.com/acaapp/acaapp2.crl*
Authority Info Access	*http://ocsp1.esfirma.com/acaapp2/* *http://ocsp2.esfirma.com/acaapp2/* *https://www.esfirma.com/doc-pki/acaapp2.crt*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F7:D4:39:1C:50:C3:42:98:9B:94:63:F8:5F:DB:BB:71:18:AC:03:A5:64:4A:3A:68:A1:83:65:AB:A5:07:9E:52*

X509SubjectName

Subject CN:	*ESFIRMA TSA 2*
Subject 2.5.4.97:	*VATES-A50878842*
Subject SERIAL NUMBER:	*A50878842*
Subject OU:	*AUTORIDAD DE CERTIFICACION ESFIRMA*
Subject O:	*ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*
Subject L:	*ZARAGOZA*
Subject C:	*ES*

X509SKI

X509 SK I	*LaYj3YePB+fYPTIf7mnkN39V9V0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2018-06-25T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

29 - TSP: SIGNATURIT SOLUTIONS, S.L.

.

TSP Name

Name	[en]	*SIGNATURIT SOLUTIONS, S.L.*
Name	[es]	*SIGNATURIT SOLUTIONS, S.L.*

TSP Trade Name

Name	[en]	*Signaturit Solutions S.L.*
Name	[en]	*VATES-B66024167*
Name	[en]	*SIGNATURIT SOLUTIONS, SL*

PostalAddress

Street Address	[en]	*Avila Street 29*
Locality	[en]	*Barcelona*
State Or Province	[en]	*Barcelona*
Postal Code	[en]	*08005*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*Calle Ávila 29*
Locality	[es]	*Barcelona*
State Or Province	[es]	*Barcelona*
Postal Code	[es]	*08005*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:legal@signaturit.com*
URI	[es]	*mailto:legal@signaturit.com*
URI	[en]	*https://www.signaturit.com/en*
URI	[es]	*https://www.signaturit.com/es*

TSP Information URI

URI	*[en]*	*https://www.signaturit.com/en/pki*
URI	*[es]*	*https://www.signaturit.com/es/pki*

29.1 - Service (granted): Sellos de tiempo cualificados emitidos por Signaturit TSA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[es]*	*Sellos de tiempo cualificados emitidos por Signaturit TSA*
Name	*[en]*	*Qualified timestamps issued by Signaturit TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *251998420895473678690910376285917392595740291 6*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGWzCCBEOgAwIBAgITcQAAASTkEGf9Sk0bGgAAAAABJDANBgkqhkiG9w0BAQsFADCBnDEYMBYG
A1UEYRMPVkFURVMtQ3Y2MDI0MTY3MSIwIAYDVQQKExlTaWduYXR1cml0IFNvbHV0aW9ucyBTLkwu
MQswCQYDVQQGEwJFUzETMBEGCzmSIomT8xxkARkWA2Nvb1TEaMBgGCzmSIomT8xxkARkWCzNpYZ25b
dHVyaXQxHjAcBgNVBAMTFVNpZ25hdHVyaXQgSXNzdWluZyBDQTAeFw0xODA3MDMwOTIxMTFaFw0y
MzA3MDIwOTIxMTFaMHgxGDAWBgNVBGEMD1ZBVEVTLUI2NjAyNDE2NzEiMCAGA1UECgwZU2lnbmF0
dXJpdCBTb2x1dGlvbnMgLUy5ML jESMBAGA1UEBwwJQmFyY2Vsb25hMQswCQYDVQQGEwJFUzEXMBUG
A1UEAwwOU2lnbmF0dXJpdCBUUlBnaGFhNAgzEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDwd41Q
z5ov9K1/EYUSE7VOSmJl4FzAfI/msMs8eVprBhUG+z+rZ0hYELzt92ph//rt97taNgc1S5lZrZ3xS
FsdSi8Af91IHOzyFnKqzDdbkWC0i0y1cEqmMJQIbWK82w7sTcgxcuWSxpd+VuUtCQhICEeCrdSHt
PUiTE4Wk0tMCxdl2nrRMNWTb9Z9tO/NPgb2Rmjx0a7nck9kGhi/m4tY8Ms99rIWvcvL TD1VTkUlbW
cnD9ptRb6gEn0Lz9t+JVcS3Xp2mUbmNKURAnNiiRFwIDZ8UUK+dpyMgPDmYRt904ZJxdCRKb17TVbCM
ePke7aHYEP90vRJqCBiGvgC8RJdBjHDAgMBAAGjggG3MIIBszAdBgNVHQ4EFgQUSKMQ5mnaw+xH
obtsNPUVJEggTt8wHwYDVR0jBBgwFoAUiq0hy7lmbDDM0tMkcIchLl66ASkwTAYDVR0fBEUwQzBB
oD+gPYY7aHR0cDovL3BraS5zaWduYXR1cml0LmNvbS9jcmwvU2lnbmF0dXJpdCUyMElzc3Vpbmcl
MjBDQS5jcmwwgZoGCCsGAQUFBwEBBIGNMIGKMFwGCCsGAQUFBzAChlBodHRwOi8vcGlpLnNpZ25h
dHVyaXQuY29tL2NlcnQvQ0EwMi5zaWduYXR1cml0LmNvbVY9TaWduYXR1cml0TTusSXNzdWluZy1y
MENBLmNydDAqBggrBgEFBQcwAYYeaHR0cDovL3BraS5zaWduYXR1cml0LmNvbS9vY3NwMAsGA1Ud
DwQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDBhBgNVHSAEWjBYMFYGCisGAQQBg4tWAwEw
SDBGBggrBgEFBQcCARY6aHR0cDovL3BraS5zaWduYXR1cml0LmNvbS9wa2kvQ1AuTGVnYWwuUmVw
cmVzZW50YXRpdmVzLnBkZANBgkqhkiG9w0BAQsFAAOCAgEAYIL XyzMTNBIUIoS MSTakilptI5nq
OGy/jk/5af2uGDZAHn/hI5eocMFQUOT9F8sSQeUwsxxDbs8Sb6Inl9hlCq7+egDAs6KwK0UE4Ggb
ElgYq7wx97S8i31cRF5xC/mTu2c4uUw6ZqMgje9gkSjyIlbYLg0Ntgir0088iNiOIXzo9/HhAfiwQ
PCbjDJTMmsnAAd884UxumWezvETCwEVYqENhQSVf6ACPyRlhmPSVej/1vsx8QmtfC4W9+1W1ojZ5
psvPV2RW7fp6n4vYWRcfxb6HSDQALcm7bUDbgHaYnA2zgcjnL0JNCT55PvO96HP77appv4Uy
7hPA1GOVVz1r/0iOFooxBMJf2l4RIy/0B0P4trQHqKmmsgQA8aYSLXpg5Ay1Ekf8S5KOFsYZfFL
LSjMg2xtfaJVgnL IvRPrsQZVJLlwpmQfcNwlrMl0CNQv6omQWWFfaPBMAcSJc20B/o5oJrNEqJNL
kZWLHpxxumxPwrzDSFkeZE6S31/9oDrAhezwpjlPlDUYJH4XxCplGvJ16uUVoLrKQ/SfX8bQUrb3
ouDVb0kUXEtDzGlF6bnykAAIDJ7zFacdB9FcTAIICLRToXoVWg/lecCb2wVwWZMnT4JB1ZOLs7gOam
ZmlN/lygqAdPWVru0J1hZ+vrXZX3j1ckY3xU4Ci7Gqo858=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Signaturit Issuing CA*
Issuer DC:	*signaturit*
Issuer DC:	*com*
Issuer C:	*ES*
Issuer O:	*Signaturit Solutions S.L.*

Issuer 2.5.4.97: *VATES-B66024167*

Subject CN: *Signaturit TSA*

Subject C: *ES*

Subject L: *Barcelona*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

Valid from: *Tue Jul 03 11:21:11 CEST 2018*

Valid to: *Sun Jul 02 11:21:11 CEST 2023*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F0:77:8D:50:CF:9A:2F:F4:AD:7F:11:85:12:13:B5:4E:4A:62:65:E0:5C:C0:7C:8F:E6:B0:CB:3C:79:5A:6B:06:15:06:FB:3F:AB:64:E8:58:10:BC:ED:F7:6A:61:FF:FA:ED:F7:BA:DA:36:07:35:4B:98:59:AF:7C:52:16:C7:52:8B:C0:1F:F7:52:07:3B:3C:85:9C:AA:B3:0D:D6:E4:58:2D:22:D3:2D:5C:12:A9:8C:25:02:1B:58:AF:36:C3:BB:13:72:0C:5C:B9:64:B1:A5:DF:95:B9:4B:42:42:12:02:11:E0:AB:75:21:ED:3D:48:93:13:85:A4:D2:D3:02:C5:D9:76:9E:B4:4C:35:64:DB:F5:9F:6D:3B:F3:4F:A9:BD:91:9A:3C:74:6B:B9:DC:93:D9:06:86:DF:E6:E2:D6:3C:32:2F:7D:AD:F5:AF:72:F2:D3:0F:55:53:91:46:D6:7A:70:FD:A6:D4:5B:1A:01:27:D0:BC:FD:B7:E2:55:73:95:E9:DA:60:E6:34:A5:11:02:73:5F:A1:11:70:0D:9F:14:50:AF:9D:A7:23:2A:3C:39:95:46:DF:74:E1:9D:71:74:24:4A:6F:5E:D3:55:B0:8C:78:F9:1E:ED:A1:D8:10:FF:74:BD:12:6A:08:17:DA:1A:F8:02:F0:12:5D:06:31:C3:02:03:01:00:01

Subject Key Identifier *48:A3:10:E6:69:DA:C3:EC:47:A1:BB:6C:34:F5:15:24:48:20:4E:DF*

Authority Key Identifier *8A:AD:21:CB:B2:26:6C:30:CC:D2:D3:24:78:87:21:2E:5E:BA:01:29*

CRL Distribution Points *http://pki.signaturit.com/crl/Signaturit%20Issuing%20CA.crl*

Authority Info Access *http://pki.signaturit.com/cert/CA02.signaturit.com_Signaturit%20Issuing%20CA.crt*

http://pki.signaturit.com/ocsp

Extended Key Usage *id_kp_timeStamping*

Certificate Policies *Policy OID: 1.3.6.1.4.1.50646.3.1*

CPS pointer: http://pki.signaturit.com/pki/CP.Legal.Representatives.pdf

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *49:77:F6:AA:EA:C4:E2:A0:45:E8:37:10:1D:CE:BA:10:A3:FE:5E:57:F7:41:55:87:FD:04:30:0F:B2:19:87:86*

X509SubjectName

Subject CN: *Signaturit TSA*

Subject C: *ES*

Subject L: *Barcelona*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

X509SKI

X509 SK I *SKMQ5mnaw+xHobtsNPUVJEggTt8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-11-22T01:00:00Z

29.2 - Service (granted): Qualified certificates issued by Signaturit Qualified Issuing CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by Signaturit Qualified Issuing CA*

Name *[es]* *Certificados cualificados emitidos por Signaturit Qualified Issuing CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *263148793345217508909437580407908006165164851 6*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIIIDCCBgigAwIBAgITdgAAAATsSDm5dwZmvAAAAAAABDANBgkqhkiG9w0BAQwFADBoMRgwFgYD
VQRhEw9WQVRFUy1CNjYwMjQxNjcxIjAgBgNVBAoTGVNpZ25hdHVyaXQgU29sdXRpb25zIFMuTC4x
CzAJBgNVBAYTAkVTMRswGQYDVQQDExJTaWduYXR1cml0IFvb3QgQ0Ew1IhcNMTkwMjA4MTQyOTAz
WhcNMjkwMjA4MTQzOTAzWjCBpjEYMBYGA1UEYRMPVkFURVMtQ0Y2MD10MTY3MSIwIAYDVQQKExlT
aWduYXR1cml0IFNvbHV0aW9ucyBTLkwuMQswCQYDVQQGEwJFUzETMBEGCgmSJomT8ixkARkWA2Nv
bTEaMBgGCgmSJomT8ixkARkWCnNpZ25hdHVyaXQxKDAmBgNVBAMTH1NpZ25hdHVyaXQgUXVhbGlm
aWVkIElzc3VpbmcgQ0IEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDmfyH0YbUEDzbZ
LOOOto5XimNbdK6w3tYs8Msa3T7nwp8+i78bRK/GUgPC6cvrV0LvY4cb1m1+z9tHvHzFidTTTLb
c3VcXOaUkxjlelnpbu3BlKLjlLLPv6lS4WexXvX4Wp4iWtmRHaenm7/rN+kcQMHfMdwObM7LqTnm
TZrTHiBtxoWWX3QwFuiMn1L4lgWO7roW4wpanKGr7ny0Rx9e8adWwKR3D4iiZpldCIW4UA1wOqXm
35qWRk6wPhdrpeHobzSHudVWIxmRN1IgyVG8ILEBT0QtKjcVWoaZEbmWLGadPnDgh/zx6uh4Sprl
mnguS/v2mP0prchtU0Q3Irr1DxT9xZvbTuerC9J+1vIZgPT13nrbhwPkPNPmstGjrB3iSO9W7/lUSHR
5YkvaGGUrG5y1Kkrh3kqvkcL+jGnttWP/I7Cj3ciW4jEdDmZGlZoiSZw3pODNOPZCHxA6TYvp/n4
tdsd1s3a3FMOVtOf4kx33Z7loym83oaYNuVerDyqHtjuIf+EOzouMagm0pO+pMllpFZRI4T52w5i
JyltE1ouF/LvnCyWAL8WyQIYX85bUY9OJ/b2U9gIlReNpvRuwApQt0GgiXq4QoyKaQ+pphv6ghX9
wcGhpV3g8Y2AaCYBgVvkGZbeOsko7HB5469RDnXbLyus5pMZfiS35Wb6cvSd9wJDAQABo4ICgCC
An4wDgYDVR0PAQH/BAQDAgGGMBAGCSsGAQQBgicVAQQDAgEBMCMGCSsGAQQBgicVAgQWBBRcb/V/
MWptdm3S4g4Wlz7L4no2MDAdBgNVHQ4EFgQUc8UKXMyak/DNxS96sBbKQKsCW9gwggEgBgNVHSAE
ggEXMIIBEzBQBgorBgEEAYOLVgIBMEIwQAYIKwYBBQUHAgEWNGh0dHA6Ly9wa2kuc2lnbmF0dXJp
dC5jb20vcGtpLi0NQLk5hdHVyYWwuUGVyc29uaCy5wZGYwVgYKKwYBBAGDi1YDATBIMEYGCCsGAQUF
BwIBFjpodHRwOi8vcGtpLnNpZ25hdHVyaXQuY29tL3BraS9DUC5MZWdlbCSSZXBvZXNlbnRhdGI2
ZXMucGRmMFEGCisGAQQBg4tWBAEwQzBBBggrBgEFBQcCARY1aHR0cDovL3BraS5zaWduYXR1cml0
LmNvbS9wa2kvQ1AuRWxlY3Ryb25pYy5TZWFscy5wZGYwCQYHBACL7EABAjAJBgcEAIvsQAEDMBkG
CSsGAQQBgicUAgQMHgoAUwB1AGIAQwBBMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAU33xS
4QbKbTDCfGeND8sdDO6LfH0wSQYDVR0fBEIwQDA+oDygOoY4aHR0cDovL3BraS5zaWduYXR1cml0
LmNvbS9jcmwvU2lnbmF0dXJpdCUyMFJvb3QlMjBDQS5jcmwwWgYIKwYBBQUHAQEETjBMMEoGCCsG
AQUFBzAChj5odHRwOi8vcGtpLnNpZ25hdHVyaXQuY29tL2NlcnQvQ0EwMV9TaWduYXR1cml0ITw
Um9vdCUyMENBLmNydDANBgkqhkiG9w0BAQwFAAOCAgEAHv6qZk9i9094vxaSSzPv67pA5GpgkKHR
BLmzSgU/1kwfjktP9ZqJxfGc+r9oGojuk2+zDRSwakJGF7B4ERxtGFXPe9k68L0/DgQZcInFqbyYO1
zC7KdF/ITox c2qUMSSB1CsZYQWzS5WaZKB45VadaNocVV04eTGgYimS8NW9wI8C24VG9uHc08/tH
JaW6MiUEkT4SOmjFLINcIci62J5m3efuptIZXcspl4r9y94Sivat29IV9rcxD0UKVrYKIJEiw3WT
Uibs3cipQULHYJ3QCD4SzXyQ+hW8IL3CMdJpXsHgxWcYm5PGhFn/cBr19k4W3W09JapUKYvNVFq
KB9mrk2uoUNvubnfDF7Y9dgMkVAzszur24dZtLyYjeE4HG9Iv WB691JzVrkiYkb/jB5NjdxU3k3
dB2gX/c2WF5MSDg5RYGoIt00b+idmOYG4GxrOFN+bLG6Pb928Q2ra7VY15JIFrDKi0GiGPsFdmf
uhn8yhyvx+I/V+sa4m4GUaebh0eUD8mk6hLBQgzyYweIroKUwwB8j6Jwio8SN5XFxz8Veg57jToB
vnt0G/SvrO9RW2xlTmM/MIbFSPyj/cQqiVfwRimMtWD5WB3/u8t0Qhjbz73opyS3m2nDzWpExhkJ
zyceQ0YGlPW7d4B+QPe7pHGDSYk4REkyD3nMo2xsd8Y=

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer CN: *Signaturit Root CA*

Issuer C:	*ES*
Issuer O:	*Signaturit Solutions S.L.*
Issuer 2.5.4.97:	*VATES-B66024167*
Subject CN:	*Signaturit Qualified Issuing CA*
Subject DC:	*signaturit*
Subject DC:	*com*
Subject C:	*ES*
Subject O:	*Signaturit Solutions S.L.*
Subject 2.5.4.97:	*VATES-B66024167*
Valid from:	*Fri Feb 08 15:29:03 CET 2019*
Valid to:	*Thu Feb 08 15:39:03 CET 2029*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:E6:7F:21:F4:61:B5:04:0F:36:D9:2C:E3:8E:B6:8E:57:8A:63:5B:74:AE:B0:DE:2B:58:C7:C3:2C:A3:74:FB:8B:0A:7C:FA:2E:FC:85:12:BF:19:48:0F:0B:A7:2F:89:58:8B:BD:8E:1C:6F:59:93:FB:3F:6B:1E:F1:F3:17:F7:53:ED:32:DB:73:75:5E:5C:E6:94:93:18:E5:7A:59:E9:6E:ED:C1:94:A2:E3:94:B2:CF:BF:A9:52:E1:67:B1:5E:F5:F8:5A:9E:22:5A:D9:91:1D:A7:A7:9B:BF:EB:37:E9:1E:40:C1:DF:31:DC:0E:6C:CE:CB:A9:39:E6:4D:9A:D3:1E:20:6D:C6:85:96:5F:74:30:16:E8:8C:9F:52:F8:96:05:8E:EE:BA:16:E3:0A:5A:9E:41:AB:EE:7C:B4:47:1F:5E:F1:A7:56:C0:A4:77:0F:88:A2:66:99:5D:0A:55:B8:50:0D:70:3A:A5:E6:DF:9A:96:46:4E:B0:3E:17:6B:A5:E1:E8:6F:34:87:B9:D5:56:23:19:91:37:52:20:C9:51:BC:20:B1:01:4F:44:2D:2A:37:15:5A:86:99:11:B9:96:2C:66:9D:3E:70:E0:87:FC:F1:EA:E8:78:4A:9A:E5:9A:08:1D:E7:26:66:3C:EA:6B:72:1B:49:25:0D:C8:AE:DD:43:C5:3F:71:66:F8:53:B9:EA:C2:F4:9F:B5:C8:86:60:3D:3D:77:9E:B6:E1:C0:F9:0F:34:F9:AC:1A:3A:C1:DE:2E:4E:F5:6E:E3:51:21:D1:E5:59:2F:68:61:94:AC:6E:72:D4:A9:2B:87:92:6A:BE:47:0B:FA:31:A7:B6:D5:8F:FE:5E:C2:8F:77:22:5B:88:C4:74:39:99:1A:56:68:89:26:70:DE:93:83:34:E3:D9:08:7C:40:E9:36:2F:A7:F9:F8:B5:DB:1D:D6:CD:DA:DC:53:0E:56:D3:9F:E3:1C:77:DD:9E:E5:A3:29:BC:DE:86:98:36:E5:5E:AC:3C:AA:1E:D8:EE:21:FF:84:3B:3A:2E:31:A8:26:D2:93:BE:A4:C9:65:A4:56:51:23:84:F9:DB:0E:62:27:29:6D:13:5A:2E:17:F2:EF:9C:2C:96:00:BF:16:C9:02:18:5F:CE:5B:51:8F:4E:27:F6:F6:53:D8:25:21:17:8D:A6:F4:6E:C0:0A:50:8B:41:A0:89:7A:B8:42:8C:8A:69:0F:A9:A6:1B:FA:81:B5:FD:C1:C1:A1:A5:5D:E0:F1:8D:80:68:26:01:81:5B:E4:7D:98:5E:3A:C9:28:EC:70:79:E3:AF:62:44:39:D7:84:BC:AE:CB:9A:4C:66:14:B7:E5:68:46:7B:14:9D:F7:02:03:01:00:01*
Subject Key Identifier	*73:C5:0A:5C:CC:9A:93:F0:CD:C5:2F:7A:B0:16:CA:40:AB:02:5B:D8*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.50646.2.1* *CPS pointer: http://pki.signaturit.com/pki/CP.Natural.Persons.pdf* *Policy OID: 1.3.6.1.4.1.50646.3.1* *CPS pointer: http://pki.signaturit.com/pki/CP.Legal.Representatives.pdf* *Policy OID: 1.3.6.1.4.1.50646.4.1* *CPS pointer: http://pki.signaturit.com/pki/CP.Electronic.Seals.pdf* *Policy OID: 0.4.0.194112.1.2* *Policy OID: 0.4.0.194112.1.3*
Basic Constraints	*IsCA: true*
Authority Key Identifier	*DF:7C:52:E1:06:CA:6D:30:C2:7C:67:8D:0C:18:9D:0C:EF:0B:7C:7D*
CRL Distribution Points	*http://pki.signaturit.com/crl/Signaturit%20Root%20CA.crl*
Authority Info Access	*http://pki.signaturit.com/cert/CA01_Signaturit%20Root%20CA.crt*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *C9:DD:26:58:A3:05:CA:25:75:1E:35:90:D5:5D:61:9A:22:AE:67:D9:98:F1:E7:E9:8A:BE:91:F6:3A:9B:2A:90*

X509SubjectName

Subject CN: *Signaturit Qualified Issuing CA*

Subject DC: *signaturit*

Subject DC: *com*

Subject C: *ES*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

X509SKI

X509 SK I *c8UKXMyak/DNxS96sBbKQKsCW9g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2019-10-01T01:00:00Z*

29.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

29.2.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.50646.2.1*

Description

29.3 - Service (withdrawn): Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description

[en] *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name *[en]* *Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"*

Name *[es]* *Servicio cualificado de entrega electrónica certificada "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *938283100535284691966*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIKqjCCCJKgAwIBAgIJMt1LNLMtxfP+MA0GCSqGSIb3DQEBCwUAMIIBIDELMAkGA1UEBhMCRVMx
DzANBgNVBAcMBk1BRFJlRDEPMA0GA1UECAwGTUFEUklEMUIwQAYDVQQLDDlzZWUgY3VvcmVudCBh
ZGRyZXNzIGF0IGhhdHBzOi8vd3d3LmNhbWVyZmlybWEuY29tLzFkZHIlc3MxLzAtBgNVBAsMKFD
IENBTUVSRkISTUEgRk9SIExFR0FMIFBFUlNPTlMgLSAyMDE2MRIwEAYDVQQFEwlBODE3NDMyODcx
GDAWBgNVBGEMD1ZBVEVTLUE4Mjc0Mzl4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMS8w
LQYDVQQDDCZBQyBDQU1FUlkzIUk1BIEZPUiBMRUdBTCBQRVJTT05TIC0gMjAxNjAeFw0yMDAxMjQw
ODE4ND1aFw0yMzAxMjMwODE4ND1aMIGiMUYwRAYDVQQDDD1TSUdOQVRVTUklUlFNPTFVUSU9OUywg
Uy5MLwgUVVBTEIGSUVEIFRSVVNUlFNFUlZJQ0VTIFBST1ZJREVSMRgwFgYDVQRhDA9WQVRFUy1C
NjYwMjQxNjcxDjAMBgNVBAsMBUxFR0FMMSEwHwYDVQQKDBhTSUdOQVRVUklUlFNPTFVUSU9OUywg
U0wxCzAJBgNVBAYTAkVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4m0Q0p9uvTj7
ld34yA4B5QxCQP+inNLoM9yOHbv+kCie6jkKRgva4PnMzaeKzK32k03oqomAB1XVuvZtbb59bnZ
vmwj4u6LEimJrqo+vorsemJrNX0rFA3ofH7OdRQ3673mNci8PdaAJwlNe0UrjAne51PrjkmdSePh
X91LURWhMcUDbJlKZJfYXhzvngREi16gsy5CazP+GIYSh5wJi0qAHbu30lo3/gaqihNjQWdWrHkk
evR169qrPGgLiEyjq2DgEaH47Hq09hoJQnqi79dEd7hv3g2TbL2pmBjT/RHKdhCiCLtXqENWiMum
zAdOahKzfISUDJuYiHbQr7PTcyuIDAQABoIFYDCCBVwwDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8E
BAMCBeAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMB0GA1UdDgQWBBSxDn20uY573wB+
H9d8MkSh6YnDTCCAX4GCisGAQQB1nkCBAIEggFuBIIBagFoAHYApLkJkLQYWBSHuxOizGdwCjw1
mATSG9+443NDsgN3BAAAAFv1qHMnAABAMARzBFAiBJ7xKNtSmMbYgzSFwTTZWXEULrR2D9P2fI
E7B0qfTU8AIbAIpbnb9NEihOJEN9DvbKmsT0LUkcTrIUqn2cn67hJqKZAHUAb1N2zDHwMRzYmQCk
URXdxUcEdkCwQApBo2yCJo32RMAAAFv1qHN+wAABAMARjBEAiAVK3P7clXg4SU6lMnU2CSTziY
sQruAx68hv3VBMO9igIgLg5c1JcaNclyQmfvi2bc1LwvRd410U2tNkEh0ZtOAcAdwDuS723dc5g
uuiFCaR+r4Z5mow9+X7By2lMAxHuJeqj9ywAAAW/Woc5VAAAAEAwBIMEYCIQDA8axPPaqZo7G24MN
zGVtpiSGBL38yqx98gTgHb4lOwIhAPlR7CFovtnQntk2qRbNYVeHRS9SBd2Hb7/Jb6vBM5lbMIGI
BgzrBgEFBQcBAQR8MHowUAYIKwYBBQUHMAKGRGhldHA6Ly93d3cuY2FtZXJmaXJtYS5jb20vY2Vy
dFMvYWNlY2FtZXJmaXJtYV9sZWdhbF9wZXJzb25zLTlwMTYuY3J0MCYGCCsGAQUFBzABhhpodHRw
Oi8vb2NzcC5jYW1lcmZpcm1hLmNvbTAfBgNVHSMEGDAWgBTDJ4WT1y+WxRusdjPZhqJKAWgUQjCB
mAYDVR0fBIGQMIGNMESgQqBAhj5odHRwOi8vY3JsLmNhbWVyZmlybWEuY29tL2FjX2NhbWVyZmly
bWFfbGVnYWxzcGVyc29ucy0yMDE2LmNybDBFoEOgQYYaHR0cDovL2Nybi0EuY2FtZXJmaXJtYS5j
b20vYWNlY2FtZXJmaXJtYV9sZWdhbF9wZXJzb25zLTlwMTYuY3JsMG0GA1UdEQRmMGSBFGxlZ2Fs
QHNpZ25hdHVyaXQuY29tpEwwSjFIMEYGCisGAQQBgYcuHgoMOENFUlRJRkIDQURPIEVMRUNUUk9O
SUNPIENVQUxJRkIDQURPIERFIFNFTExPIEVMRUNUUk9OSUNPMBwGA1UdEgQVMBOBEWNhQGNhbWVy
ZmlybWEuY29tMIHUBgNVHSAEgcwwgckwgbsGDSsGAQQBg YcuChACAQIwgakwKQYIKwYBBQUHAgEW
HWhldHBzOi8vcG9saWN5LmNhbWVyZmlybWEuY29tMHwGCCsGAQUFBwICMHAMbkNlcnRpZmljYWRv
IGN1YWxpZmlj YWRvIGRlIHNlbGxvIGVsZWN0cm9uaWNvLiBDb25zdWx0ZSBsYXMgY29uZGljaW9u
ZXMgZGUgdXNvIGVuIGhtdHBzOi8vcG9saWN5LmNhbWVyZmlybWEuY29tMAkGBwQAr+xAAQEwgdAG
CCsGAQUFBwEDBHIDMDIHAAMxgGBgQAjkYBATALBgYEAI5GAQMCAQ8wgZEGBgQAjkYBBTCBhjBBFjto
dHRwczovL3Bkcy5jYW1lcmZpcm1hLmNvbS9kb2NzL1BEU19MZWdhbF9QZXJzb24tdjEuMEVOLnBk
ZhMCZW4wQRY7aHR0cHM6Ly9wZHMuY2FtZXJmaXJtYS5jb20vZG9jcy9QRFNfTGVnYWxfUGVyc29u
LXYsLjBFUy5wZGYTAmVzMBMGBgQAjkYBBjAJBgcEAI5GAQYCMA0GCSqGSIb3DQEBCwUAA4ICAQB0
1Lk4fU7kzfIbV3MGr/jkYB/FKXvSzaZAmdhjlKBkzJIFOFzc17GOmu2zBSjMlL/ksSY266qcXZ
lxER4R/yz3aTq2gikJ/NahYvTSOoevURHGMtDsTqzJ3e/zmi/+fwMnElbsRq5IYXMGGH6n3+OVrN
j9N93I5apSCKjQxn3dBeXLAtif2q2qsPWEu+LFuefVBBwCUwFmXMGnTWuk0L/q70gGpvA0K9CAqV
4yuEMbYSr2fyFSpogHJZnjAJ+MSWLKjqx++oEjIDYHMVIH347essgyuGpa5Kq1m81sDGMvJ03a43s
L7CYVxq+iOkdgKi7XAQHezFIvdLpq51GV/DIlhZ/L2NsoIEyzekqSHgwPluSnoHR8tm6xVL5/Lc
76mirj7pl/9fO4ftxxzQ2e+HjUI40TlyMp3Z+SgT543Dpm9GIhTZ24RYLtPSjsAqbf8aQb gVUqtl
q2Mjpcd2GIETOaK2hlLS5cqML5yIu9Ni1NCAvysrR+/lgRjGnQeR+25V2izm3pPJF88GJ2r1/uEp
X3sKloly5OCARUEJ1TPpk9eC0yxjpgYb1vGSQkAXNeDCmElSyz13X/soTPkoCyjXyk7zfibdlneK
vp8Tv788k4vW4Yz3lEWyFxcowg7DI biPk8hmH77YIs55g3WHXNeZmJi+eLTpX+d0kdutXhdSBg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Issuer OU:	*see current address at https://www.camerfirma.com/address*
Issuer ST:	*MADRID*
Issuer L:	*MADRID*
Issuer C:	*ES*
Subject C:	*ES*
Subject O:	*SIGNATURIT SOLUTIONS, SL*
Subject OU:	*LEGAL*
Subject 2.5.4.97:	*VATES-B66024167*
Subject CN:	*SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER*
Valid from:	*Fri Jan 24 09:18:42 CET 2020*
Valid to:	*Mon Jan 23 09:18:42 CET 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E2:6D:10:D2:9F:6E:BD:38:FB:95:DD:F8:C8:0E:01:E5:0B:C2:40:FF:A2:9C:D2:E8:33:DC:8E:1E:1B:FE:90:28:9E:EA:39:0A:46:0B:DA:E0:03:E7:33:36:9E:2A:B2:B7:DA:43:B7:A2:AA:26:00:1D:57:56:EB:D9:B5:B8:79:F6:19:D9:BE:6C:23:E2:EE:8B:12:29:89:AE:AA:3E:BE:8A:EC:7A:62:6B:35:7D:2B:14:0D:E8:7C:7E:CE:75:14:37:E9:3D:E6:35:C8:BC:3D:D6:80:27:09:4D:7B:45:2B:8C:09:DE:E7:53:EB:8E:49:9D:49:E3:E1:5F:DD:4B:51:15:A1:31:C5:03:6C:99:4A:64:97:D8:5E:1C:EF:9E:04:44:8B:5E:A0:B3:2E:42:6B:33:FE:18:86:39:87:9C:09:8B:4A:80:1D:BB:B7:D2:5A:37:FE:06:AA:8A:13:63:41:67:56:AC:79:24:7A:F4:75:EB:DA:AB:3C:68:0B:88:4C:A3:AB:60:E0:11:A1:F8:EC:7A:B4:F6:1A:09:42:7A:A2:EF:D7:44:77:B8:6F:DE:0D:93:6C:BD:A9:98:18:D3:FD:11:CA:76:10:A2:08:B8:97:A8:43:56:88:CB:A6:CC:07:4E:6A:12:A0:1D:25:03:0E:E4:E2:1E:14:2D:EC:F4:DC:8F:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Extended Key Usage	*id_kp_clientAuth*
Subject Key Identifier	*B1:0E:7D:B4:B9:8E:7B:DF:00:7E:1F:D7:7C:B4:C9:12:87:A6:27:0D*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt* *http://ocsp.camerfirma.com*
Authority Key Identifier	*C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl* *http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl*
Subject Alternative Name	*legal@signaturit.com* *OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO*
Issuer Alternative Name	*ca@camerfirma.com*

Certificate Policies	*Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2* *CPS pointer: https://policy.camerfirma.com* *CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]* *Policy OID: 0.4.0.194112.1.1*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*E1:89:8C:7B:47:8C:21:F3:CB:45:48:D7:A6:CA:F5:AC:F2:C9:DE:B5:6D:9D:70:65:BA:B2:E1:4D:1E:3D:BD:14*

X509SubjectName

Subject C:	*ES*
Subject O:	*SIGNATURIT SOLUTIONS, SL*
Subject OU:	*LEGAL*
Subject 2.5.4.97:	*VATES-B66024167*
Subject CN:	*SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER*

X509SKI

X509 SK I	*sQ59tLmOe98Afh/XfLTJEoemJw0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-07-01T01:00:00Z

29.3.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name	*[en]*	*Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"*
Name	*[es]*	*Servicio cualificado de entrega electrónica certificada "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject O:	*SIGNATURIT SOLUTIONS, SL*
Subject OU:	*LEGAL*
Subject 2.5.4.97:	*VATES-B66024167*
Subject CN:	*SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER*

X509SKI

X509 SK I	*sQ59tLmOe98Afh/XfLTJEoemJw0=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2020-06-15T22:00:00Z*

30 - TSP: IVNOSYS SOLUCIONES S.L.U.

.

TSP Name

Name	*[es]*	*IVNOSYS SOLUCIONES S.L.U.*
Name	*[en]*	*IVNOSYS SOLUCIONES S.L.U.*

TSP Trade Name

Name	*[en]*	*IVNOSYS*
Name	*[en]*	*IVNOSYS SOLUCIONES S.L.*
Name	*[en]*	*VATES-B98333362*
Name	*[es]*	*VATES-B98333362*

PostalAddress

Street Address	*[en]*	*C/Acceso Ademuz 12-1º-Oficina 1*
Locality	*[en]*	*Paterna*
State Or Province	*[en]*	*Valencia*
Postal Code	*[en]*	*46980*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*C/Acceso Ademuz 12-1º-Oficina 1*
Locality	*[es]*	*Paterna*
State Or Province	*[es]*	*Valencia*
Postal Code	*[es]*	*46980*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:administracion@ivnosys.com*
URI	*[es]*	*https://www.ivnosys.com*
URI	*[es]*	*mailto:administracion@ivnosys.com*

URI	*[en]*	*https://www.ivnosys.com*

TSP Information URI

URI	*[en]*	*https://www.ivnosys.com/en/*
URI	*[es]*	*https://www.ivnosys.com/es/*

30.1 - Service (granted): Qualified Certificates issued by IVSIGN CA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by IVSIGN CA*
Name	*[es]*	*Certificados cualificados emitidos por IVSIGN CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3579684697560397415*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJTDCCBzSgAwIBAgIIMa2YRDX9NmcwDQYJKoZIhvcNAQELBQAwggEMMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFk
ZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9G
IENPTUJlTUkNFIFJPT1QgLSAyMDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVT
LUE4Mjc0MzI4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSkwJwYDVQQDDCBDSEFNQkVS
UyBPRiBDT01NRVJDRSBST09UIC0gMjAxNjAeFw0xNzEwMDUxMDA5MjBaFw00MDAzMTYxMDA5MjBa
MIGxMQswCQYDVQQGEwJFUzEQMA4GA1UEBwwHUEFURVJOQTFAMD4GA1UECww3c2VlIGN1cnJlbnQg
YWRkcmVzcyBhdCBodHRwczovL3BzZWMuaXZub3NScy5jb20vYWRkcmVzczEYMBYGA1UEYQwPVkFU
RVMtQk4MzAzMzYyMSAwHgYDVQQKDBdJVkSPU1lTIFNPTVDSUS0ORVMgUy5MLjESMBAGA1UEAwwJ
SVZTSUdOIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA1ssEV7kgGc4/pNlrehXv
Bbv3TP7qNZi8tfGCeXjJzvsMt0FVh3nKcUIcVCYJEptrOgZvat/E+RXkJTjZWZ/AgcaYT7WKlIC6
Dv9N/B0PUZvXdlNrWWgDwBU8qKROO6E2wdCv1W/AasIduOFotdhE8BYxiZMyDWtBluqgavSw5Z
UkTZic3+bFYgEO4nfKH+1dvr7JxMlPoBTbpbBgGH0QC9Pds6uR1ibuNp69kA23oyORmf+bNGSR
qVxkeF51KooE24cdz6xnzSPgAjo0Hfb3dT4sStcVe+I6PvrUh1Bc1o5zarmbVbO5tq1ww4Fiq2lc
HAkoWZR46qGvVyBOrJMOh+jNVm90F/I30g/dc1rf3pacsLpt02dQl0LD6b0W/bhwNMGlnSj35g1U
HGPG4zPrvBhtFy1pJvXNaeHyAD4fKthg17SILK1IPCVubZCWxEcB3NOTVZejdG02G6lsTuQrAz
QztITw7zN1wCtEvi5yPnG9XRXg/0VMoicofdf+YzFiOGYv2z8FHtcR8espHYrSpvIr6dFZjZiRtN
rfUvQcyhWhSIRoqOqFCErKuZhXuFlWGunZUDnhBLnLmiaWkGRWNlRkTQgfOsT3vyYV8mtYW78sd/
TZEzyauOcJaPDUi8wxrZ+W1mi0NrY6JvDy+XtOEA0gsQCGsYKL86dS0CAwEAAaOCAwgwggMEMBIG
A1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFAUtYvSbyP1iJPkmjCE1Hz0ufBlKMIIBRQYDVR0j
BIIBPDCCATAFJ4uZUS+V/WrzZbGi9+zNWTK6J6LoYIBFKSCARAwggEMMQswCQYDVQQGEwJFUzEP
MA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFk
ZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENlQU1CRVJTIE9G
IENPTUJlTUkNFIFJPT1QgLSAyMDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVT
LUE4Mjc0MzI4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSkwJwYDVQQDDCBDSEFNQkVS
UyBPRiBDT01NRVJDRSBST09UIC0gMjAxNjAiNlJNAto1YGsrMvgYMGCCsGAQUFBwEBBHcwdTBLBggr
BgEFBQcwAoYaHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9jaGFtYmVyc29mY29tbWVy
Y2Vyb290LTlwMTYuY3J0MCYGCCsGAQUFBzABhhpodHRwOi8vb2Nzcc5jYW1lcmZpcm1hLmNvbTAO
BgNVHQ8BAf8EBAMCAQYwHQYDVR0lBBYwFAYIKwYBBQUHAgEWHfWbldHBzOi8vaWN5LmNhbWVyZmlybWEuY29tMIGO
NQYGZ4EMAQICMCswKQYIKwYBBQUHAgEWHfWbldHBzOi8vaWN5LmNhbWVyZmlybWEuY29tMIGO
BgNVHR8EgYYwgYMwP6A9oDuGOWh0dHA6Ly9jcmwuY2FtZXJmaXJtYS5jb20vY2hhbWJlcnNvZmNv
bW1lcmNlcm9vdC0yMDE2LmNybDBAoD6gPIY6aHR0cDovL2NybDEuY2FtZXJmaXJtYS5jb20vY2Hh
bWJlcnNvZmNvbW1lcmNlcm9vdC0yMDE2LmNybDANBgkqhkiG9w0BAQsFAAOCAgEAj8MPLwP/YtQU
nvbl/puJOuogI6CBnK1acSSnn9TH0J8WUsnBCoZNJ7nM7m/8B9hEIaPumgzEaQyt7i3McIGq9mS06o
ZHPAPb8Jbd0QVBQUeAvKD81UtG2QFzQ7dmoYydz3ZNBujzJsVqs+fp4ODc7uX8dYEWw0lkVcPJ+3
AsA5n+LZJjlIzfnoDwnohclPBs0vZY8QLz8hZuiMYIG+vh9W0u8UdiOQL7mOlYdojdQyM8tIjhdX
qSoBHpDeIbGJIBVo/rX1R/pXFXMg102rUI1OyO6Zb34+yRtVJ4JUhpPuQNvKk8iMcVrA6IA3z
+vJTVkIZNkST6:7IAwkfps7mvWD+UJwVuAB0GOquoudqNcYdzCTCtpkGTjXSu1BQd6bMzHdL18j
llhJ24CHEuaLcARJK8idGtOPbPVZQRMZiZ2SoytC+nhXaYCcznGOMSNqJYuT20hVIZorMfxJPWTA
WmPB/FVdqoea/GcFIcP6D+L7T+QUyEKdi5qPAIT2jnJc2QolorN2spjEU4lPu+E/n4rfAMzpGGUz
sJ58Ai73j/TpKwdnauu9WWObXnrYbfT0C+a78QjLA3gd9iNMZRS+tMBsWjNDvzjHOvhVvgnjyCZq
HJ6Pl4kV1TKfi2vhFzrEpvXoZuzMocNqSyy6S7v03hz0nGB7oxQpnFxLQUsuIY=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*CHAMBERS OF COMMERCE ROOT - 2016*
Issuer O:	*AC CAMERFIRMA S.A.*

Issuer 2.5.4.97:	*VATES-A82743287*
Issuer SERIAL NUMBER:	*A82743287*
Issuer OU:	*CHAMBERS OF COMMERCE ROOT - 2016*
Issuer OU:	*see current address at www.camerfirma.com/address*
Issuer L:	*MADRID*
Issuer ST:	*MADRID*
Issuer C:	*ES*
Subject CN:	*IVSIGN CA*
Subject O:	*IVNOSYS SOLUCIONES S.L.*
Subject 2.5.4.97:	*VATES-B98333362*
Subject OU:	*see current address at https://psec.ivnosys.com/address*
Subject L:	*PATERNA*
Subject C:	*ES*
Valid from:	*Thu Oct 05 12:09:20 CEST 2017*
Valid to:	*Fri Mar 16 11:09:20 CET 2040*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D6:CB:04:57:B9:20:19:CE:3F:A4:D9:6B:7A:15:EF:05:BB:F7:4C:FE:EA:35:98:BC:B5:F1:82:79:78:C9:CE:FB:0C:B7:41:55:87:79:CA:71:42:1E:54:26:09:12:9B:6B:3A:06:6F:6A:DF:C4:F9:15:E4:25:38:D9:59:9F:C0:81:C6:98:4F:B5:8A:96:50:BA:0E:FF:4D:FC:1D:0F:51:9B:D6:C6:59:4D:AD:65:A0:0F:00:54:F2:A2:91:38:EE:84:DB:07:42:BF:55:BF:01:AB:25:76:E3:85:A2:D7:61:13:C0:58:C6:26:4C:C8:35:9F:06:5B:AA:AA:36:AF:4B:0E:59:52:4E:D9:89:CD:FE:6C:56:2A:10:EE:27:74:A1:FE:D5:DB:EB:EC:9C:4C:94:FA:01:4D:BA:5B:06:01:87:D1:00:BD:3D:DB:3A:B9:17:FF:25:BB:8D:A7:AF:64:03:6D:E8:C8:E4:66:7F:FF:9B:34:64:91:A9:5C:64:78:5E:75:2A:8A:04:DB:87:1D:CF:AC:67:CD:23:E0:02:3A:34:1D:F6:F7:75:3E:2C:4A:D7:15:7B:E2:3A:3E:FA:D4:87:50:5C:D6:8E:73:6A:B9:9B:55:B3:B9:B6:AD:70:C3:81:63:AB:6B:5C:1C:09:28:59:94:78:EA:A1:AF:57:20:4E:AC:93:0E:87:E8:CD:56:6F:74:17:F2:37:D2:0F:DD:73:5C:DF:DE:96:9C:88:BA:6D:D3:67:50:97:42:C3:E9:BD:16:FD:B8:70:34:C1:88:9F:C8:F7:E6:0D:54:1C:63:C6:E3:37:CF:BC:16:E2:7C:5C:B5:A4:9B:D7:35:A7:87:C8:00:F8:7C:AB:61:83:5E:D2:24:B2:B5:20:F0:95:B9:B6:7F:09:6C:44:78:1D:CD:39:35:59:7A:37:46:D3:61:BA:22:C4:EE:42:B0:33:43:3B:48:4C:8C:13:AC:DD:70:0A:D1:2F:8B:9C:8F:C8:6F:57:45:78:3F:D1:53:28:FD:CA:34:74:8F:93:AC:5D:06:57:6C:FC:16:21:ED:FD:1F:1E:B2:91:D8:AD:2A:6F:22:BE:22:15:98:F6:89:1B:4D:AD:F5:2F:41:CC:A1:5A:14:A5:46:8A:8E:A8:50:84:AC:AB:99:85:7B:85:95:61:AE:9D:95:03:9E:10:4B:9C:B9:A2:69:69:06:45:63:65:46:44:D0:81:F3:AC:4F:7B:F2:61:5F:26:B5:85:BB:F2:C7:7F:4D:91:33:C9:AB:8E:70:96:8F:0D:48:BC:C3:1A:D9:F9:6D:66:8B:43:6B:63:A2:6F:0F:2F:97:B4:E1:00:D2:0B:10:08:6B:18:28:BF:3A:75:2D:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*05:2D:62:F4:9B:C8:FD:62:24:F9:26:8C:21:35:1F:3D:2E:7C:12:0A*
Authority Key Identifier	*9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*
Authority Info Access	*http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt* *http://ocsp.camerfirma.com*
Extended Key Usage	*id_kp_clientAuth*
Certificate Policies	*Policy OID: 2.23.140.1.2.2* *CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points	*http://crl.camerfirma.com/chambersofcommerceroot-2016.crl* *http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *92:19:3F:42:7D:FD:45:D1:F7:EE:0C:0A:3B:1A:97:4E:A7:AF:76:79:18:39:90:E2:87:62:C1:3A:26:3D:B9:78*

X509SubjectName

Subject CN: *IVSIGN CA*

Subject O: *IVNOSYS SOLUCIONES S.L.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *see current address at https://psec.ivnosys.com/address*

Subject L: *PATERNA*

Subject C: *ES*

X509SKI

X509 SK I *BS1i9JvI/WIk+SaMITUfPS58Ego=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2019-10-28T01:00:00Z

30.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

30.1.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3*
Description		

30.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*Qualified Certificates issued by IVSIGN CA*
Name	*[es]*	*Certificados cualificados emitidos por IVSIGN CA*

Service digital identities

X509SubjectName

Subject CN:	*IVSIGN CA*
Subject O:	*IVNOSYS SOLUCIONES S.L.*
Subject 2.5.4.97:	*VATES-B98333362*
Subject OU:	*see current address at https://psec.ivnosys.com/address*
Subject L:	*PATERNA*
Subject C:	*ES*

X509SKI

X509 SK I	*BS1i9JvI/WIk+SaMITUfPS58Ego=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-11-22T01:00:00Z*

30.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

30.1.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3

Description

30.2 - Service (granted): Certificados Cualificados emitidos por IvSign Global CA

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Certificados Cualificados emitidos por IvSign Global CA

Name [en] Qualified Certificates issued by IvSign Global CA

Service digital identities

Certificate fields details

Version: 3

Serial Number: *379154344366198274416 9*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHxTCCBa2gAwIBAgIKAM2KPEGNbcc+aTANBgkqhkiG9w0BAQsFADCBkDELMAkGA1UEBhMCRVMx
ETAPBgNVBAgTCFZBTEVOQ0lBMRcwFQYDVQQLEw5UUlVTVCBTRVJWSUNFUzEYMBYGA1UEYRMPVkFU
RVMtQjk4MzMzMzYyMSIwIAYDVQQKExlJVk5PU1lTIFNPTFVDSU9ORVMgUy5MLlUuMRcwFQYDVQQD
Ew5JdlNpZ24gUm9vdCBDQTAeFw0yMDA5MTEwOTU5MzNaFw0zMjA5MTEwOTU5MzNaMIGSMQswCQYD
VQQGEwJFUzERMA8GA1UECAwIVkFMRUlDNSIxFzAVBgNVBAsMDlRSVVNUIFNFUZIQ0VTMRgwFgYD
VQRhDA9WQVRFUy1COTgzMzMzNjIxIjAgBgNVBAoMGUlWTk9TWVMgU09MVUNJTO5FUyBTLkwuVS4x
GTAXBgNVBAMMEEl2U2InbiBHbG9yYWwgQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoIC
AQC12RHSzGEKI3UNJT21LXBHBANZcA1AVh5vsHcO0aLPN2/7IfxXYUd4hFEv3NvDtanSu3sSCcEb
UqZ4h4J2LVTkWO9yRSZ6sGl8Cd8VMdgYJRzDVoMOau1qrQLMPHRly3oVTV6yCe26FBsn3il1vb2V
pcnI1AuiK5v9V0VbQn05fKMo3vfO2UdbsPZ6NT+OsuHtF7kC+X5NPuSjOVxYerLegykUFLjRX3
t/m75dDCvSG+JoZotkq2+HwxUUTEXlFEefeLN4UG4jY9KhheUFQ8KVs8uixKjwInsOgUlR57N6nf
nPd5WSIkh5qcbkXuChgDCbNroCcMfnX+fmT5ZXfRMdou2Qvyh5729grIp9zMidNfB1lZ4ayfaBp
9kaj37gCkOv4FhkrEVXPmLBXQUquvFlIV2coe/3y8OzM151bbQ9xzs6zFHKKAGFJSoQ/T4/1P+Q9M
cVKL0ljuyg3+xh3HGcpNPVseSqpokkIH03KYKw8PhGK6oC5CExL9vSL16Wv1zIkA1MFMdD+Dt
WN5FYq7nGAZYnQPMDnEw6/gWBAy2Chp+E3UXdouO4RZmahXbw5GKqFxUEJ9aULGvPf+pCtbCbFPu
u13xkX+a3TSllcgs4G6nVl9mC8oDX+9eEyHyxHnaXW9yJp4shdAAZCBoHHOj3TcmhcH+eGbRFWUe
twIDAQABo4ICGzCCAhcwEgYDVR0TAQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQU6mFaLpsfvPgpDPrE
3pLH1To4xMjMwIwYDVR0jBBgwFoAUONBV+FkrEIMIREiKL3ADSKGcAEx4wg2IGCCsGAQUFBwEBBIGF
MIGCMDcGCCsGAQUFBzAChitodHRwOi8vY2EuaXZraWduLmNvbS9ZXJ0cy9pdnNpZ25yb290Y2Eu
Y3J0MCIGCCsGAQUFBzABhhZodHRwOi8vb2NzcC5pdnNpZ24uY29tMCMGCCsGAQUFBzABhhododHRw
Oi8vb2NzcDluaXZraWduLmNvbTCBtgYDVR0gBIGuMIGrMIGoBgRVHSAAMIGfMCUGCCsGAQUFBwIB
FhodHRwczovL3BvbGlpcS5pdnNpZ24uY29tMHYGCCsGAQUFBwICMGoaaEI2U2InbiBHbG9bYWwg
Q0EuIENlcnRpZmlpYXRpb24gUHJhY3RpY2UgU3RhdGVlZW50cyBhbmQgQ2VvdGlmaWNhdGUgUG9s
aWNpZXM6lGh0dHBzOi8vcG9saWN5Lml2bm9zeXMuY29tMGMGA1UdFwRcMFowK6ApoCeGJWh0dHA6
Ly9jcmwxLml2c2Inbi5jb20vaXZzaWduem9vdC5jcmwwK6ApoCeGJWh0dHA6Ly9jcmwyLml2c2ln
bi5jb20vaXZzaWduem9vdC5jcmwwDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3DQEBCwUAA4ICAQBc
/ts3nEz2i+i3XyUFIR/NWbstY784IXw1fpDX5PPqG3N9AJhmI/8DIDZvgF7p1Tvef5fgkY9wFNch+9
T1dezu3HWWCapVKsIQ9My9/VCWIC8/++oMt8i0YjNJde7sSpcW/RSxwAcBtbxjoi1Y0G2NmW0hPc
MIEqLxR7VgdrirOjou4nFIwdv2Ypmr+gwKkHDqwtEITe9ZrklpthKokmXKOiQHcLQsNlxOELh8SA
VO2Wcf+MKGIH78gyuAdQ1kt5iFd8DaYwKDJa0pYBhm1JVOepAPNv54YRKRTMARthg1HieWcgYCdv
tuwKG06MtqmQNWYYiEHIHs/xzk/ThMUS/CelkyPH31IG6KjbA3Bj3KS03VVY6tIRuo5ghIhm36k1
ysS7Zquhhr4taKdUY7G8FQWjlU5CDA/RdA/iOcxBK+iQTg8gUQhhwtJc845guOYIfEd1RBjHYojI
wW0IQWABN3mzpcMvTz7nbdf1kVizM+PdKfw//1xPXBRB07CYkDbywT9DE7ZvlsRQ3LjdmZCb/Aee
d9hhW1vNpJZ5ASgHC3DvbmzE2b+Twg3lBQIxN0v4ms2n0gITB7XUWhETOSxCYy5gF/ylp1TBYAJ6
NFoYS+wx2V6N/0I5tspWr1suBEXvoM+rYXHe6IDuuH7qh0PSd7I0zSCD+AxJTOTHLxG16DeQ8g==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *IvSign Root CA*

Issuer O: *IVNOSYS SOLUCIONES S.L.U.*

Issuer 2.5.4.97: *VATES-B98333362*

Issuer OU: *TRUST SERVICES*

Issuer ST: *VALENCIA*

Issuer C: *ES*

Subject CN: *IvSign Global CA*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *TRUST SERVICES*

Subject ST: *VALENCIA*

Subject C: *ES*

Valid from: *Fri Sep 11 11:59:33 CEST 2020*

Valid to: *Sat Sep 11 11:59:33 CEST 2032*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B5:D9:11:D2:CC:61:0A:97:75:0D:25:3D:B5:2D:70:47:04:03:59:70:0D:40:56:1E:6F:B0:77:0E:D1:A2:CF:37:6F:FB:2
1:FC:57:61:47:78:84:51:2F:DC:DB:C3:B5:A9:D2:BB:7B:12:09:E1:1B:52:A6:78:F3:82:62:D8:B5:53:91:63:BD:C9:14:99:9C:69:7C:09:DF:15:31:D8:18:21:1C:C3:56:83:0E:6A:2D:6A:AD:02:CC:3C:74:48:CB:7A:15:21:5E:B2
:09:ED:BA:14:1B:27:DE:29:75:BD:BD:95:A5:E9:C8:20:0B:62:47:7B:FD:57:45:5B:89:09:CE:E5:F2:8C:A0:9C:1F:3B:65:1D:6E:C3:FF:67:A3:53:F8:EB:2E:1E:D1:7B:90:2F:97:E4:D3:EE:4A:33:95:C5:87:AB:2E:B8:32:91:41
:4B:8D:15:F7:B7:F9:BB:E5:D0:C2:BD:21:BE:26:86:68:B6:4A:B6:F8:7C:31:51:44:C4:5E:51:44:79:F7:8B:37:85:06:E2:36:3D:2A:18:5E:50:54:3C:29:5B:3C:BA:2C:4A:8F:09:67:B0:E8:14:95:1E:7B:37:A9:DF:9C:F7:79:59:22
:24:87:9A:9C:6E:45:EE:0A:18:03:09:B3:6B:A0:27:0C:7E:75:FE:7E:64:F9:65:77:D1:31:DA:2E:D9:0B:F2:87:9E:F6:F6:0A:F5:A7:DC:FF:32:27:4D:7C:1D:48:67:86:B2:7D:A0:69:F6:46:A3:DD:38:02:90:EB:F8:16:19:2B:11:5
5:CF:98:B0:57:41:44:2E:BC:59:48:57:67:28:7B:FD:F2:F0:E8:8C:D7:9D:5B:6D:0F:71:CF:AC:C5:1C:A2:80:18:52:52:A1:0F:D3:E3:FD:4F:F9:0F:4C:71:52:8B:D2:58:EE:CA:0D:FE:C6:1D:C7:19:EA:4D:3D:5B:1E:F1:CA:68:
92:42:07:D3:72:98:2B:0F:0F:88:62:BA:B8:2E:42:12:F2:FD:BD:22:C8:FF:A5:AF:27:32:09:90:09:75:30:53:1D:0F:E0:E2:58:DE:45:62:AE:E7:18:06:58:9D:03:CC:0E:71:30:EB:F8:16:04:0C:B6:0A:1A:7E:13:75:17:76:8B:8E:E
1:16:66:6A:15:DB:C3:91:8A:A8:5C:54:10:9F:5A:50:B1:AF:3D:FF:A9:0A:D6:C2:6C:53:EE:BB:5D:F1:91:7F:9A:DD:34:A5:21:C8:2C:E0:6E:A7:56:5F:66:0B:CA:03:5F:EF:5E:13:21:F2:C4:79:DA:5D:6F:72:26:9E:2C:85:D0:
00:64:20:68:1C:73:A3:DD:37:26:85:C1:FE:78:66:D1:15:65:1E:B7:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33*

Authority Key Identifier	*38:D0:55:F8:59:2B:12:53:08:44:48:8A:2F:70:03:49:71:80:13:1E*
Authority Info Access	*http://ca.ivsign.com/certs/ivsignrootca.crt* *http://ocsp.ivsign.com* *http://ocsp2.ivsign.com*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://policy.ivsign.com* *CPS text: [IvSign Global CA. Certification Practice Statements and Certificate Policies: https://policy.ivnosys.com]*
CRL Distribution Points	*http://crl1.ivsign.com/ivsignroot.crl* *http://crl2.ivsign.com/ivsignroot.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D6:EA:13:D3:B7:70:57:17:E3:AD:56:07:3B:1A:9D:DE:00:57:97:60:3B:9A:A7:3A:71:04:48:E9:62:F5:41:C5*

X509SubjectName

Subject CN:	*IvSign Global CA*
Subject O:	*IVNOSYS SOLUCIONES S.L.U.*
Subject 2.5.4.97:	*VATES-B98333362*
Subject OU:	*TRUST SERVICES*
Subject ST:	*VALENCIA*
Subject C:	*ES*

X509SKI

X509 SK I	*6mFaLpsfvPgpDPrE3pLHTu4xMjM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-03-17T01:00:00Z

30.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

30.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

30.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.4.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.6.4.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.6.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.1.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.1.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.2.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.3.3

Description

30.3 - Service (granted): Qualified electronic registered delivery service ”SERVICIOS ELECTRONICOS DE CONFIANZA – IVNOSYS”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description

[en] *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name *[en]* *Qualified electronic registered delivery service ”SERVICIOS ELECTRONICOS DE CONFIANZA – IVNOSYS”*

Name *[es]* *Servicio cualificado de entrega electrónica certificada ”SERVICIOS ELECTRONICOS DE CONFIANZA – IVNOSYS”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1201545153274936677250*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIKjCCCA6gAwIBAgIQSLJ5tgw4dOCMA0GCSqGSIb3DQEBCwUAMIIBIDELMAkGA1UEBhMCRVMx
DzANBgNVBAcMBk1BRFJJRDEPMA0GA1UECAwGTUFEUkIEMUIwQAYDVQQLDDlzZWUgY3VycmVudCBh
ZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2FkZHIlc3MxLzAtBgNVBAsMIkFD
IENBTUVSRkISTUEgRk9SIExFR0FMIFBFUlNPTlMgLSAyMDE2MRIwEAYDVQQFEwlBODE3NDMyODcx
GDAWBgNVBGEMD1ZBVEVTLUE4Mjc0Mzl4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMS8w
LQYDVQQDDCZBQyBDQU1FUlkZIUk1BIEZPUiBMRUdBTCBORVJTT05TIC0gMjAxNjAeFw0xOTEyMTAx
NjU4MjIaFw0yMzEyMDkxNjU4MjIaMIG4MUEwPwYDVQQQDDb1TRVJWSUNJTTMgRUxFQ1RST05JQ09T
IERFIENPTkZJQU5aQSAtIEIWTk9TWVMgU09MVUNJT05FUzEYMBYGA1UEYQwPVkFURVMtQjk4MzMz
MzYyMRUwEwYDVQQLDAxESVJFQ0NJT04gSVQxETAPBgNVBAsMCEdFUkVOQ0lBMSIwIAYDVQQKDBlJ
VkSPU1ITIFNPTFVDSU9ORVMgUy5ML1UuMQswCQYDVQQGEwJFUzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALKXmEDrqmJ7DLuvd/1dGKdMTI7ldhn2AIZ2pAfuzmvZqC7kFIC2+6kc9j8i
Ij86h1/4KzG2bzKsBko5UQobTYUMX9wJWv6QZlZKAmF/wtostcN4RaŘzJLwkzzntMKk9rb0cnxfV
bKgC3Pss3RWLBoAyyAi6b1ou1mGR5ZEnxmnxvshDCqeoahFsS4ezNNuS447dboilCS2/7KkIsWlI
j07UTGmOUCIHvA/HqoRwaHPt2osQ02unCXqqC8EbCb0sntJmSrFIksbrGAsYCLGSPa2i/z4W9lQS
Z8pa5C8kAosHZWprTuGxR+pKfzOfcRlanuCSC94TI7zTLeuEJXKZ8kCAwEAAaOCBMYwggTCMAwG
A1UdEwEB/wQCMAAwDgYDVR0PAQH/BAQDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
BDAdBgNVHQ4EFgQUrakGqaqA9UdbK5VtS3EHT21jH5EwgYgGCCsGAQUFBwEBBHwwejBQBggrBgEF
BQcwAoZEaHR0cDovL3d3dy5YW1lcmZpcm1hLmNvbS9jZXJ0cy9hY19YW1lcmZpcm1hX2xlZ2Fs
X3BlcnNvbnMMjAxNi5jcnQwIgYIKwYBBQUHMAGGGmhtdHA6Ly9vY3NwLmNhbWVyZmlybWEuY29t
MIIBRQYDVR0jBIIBPDCCATAFMMnhZPXL5bFG6x2M9mGokp9aBRCoYIBFKSCARAwggEMMQswCQYD
VQQGEwJFUzEPMA0GA1UECAwGTUFEUkIEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBj
dXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxKTAnBgNVBAsMIENI
QU1CRVJTIE9GIENPTU1FUkNFIFJPT1QgLSAyMDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGDAWBgNV
BGEMD1ZBVEVTLUE4Mjc0Mzl4NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSkwJwYDVQQD
DCBDSEFNQkVSUyBPRiBDT01NRVJDRSBST09UIC0gMjAxNoIIVLFu4REkWk1wgZgGA1UdHwSBkDCB
jTBEoEKgQIY+aHR0cDovL2NybC5jYW1lcmZpcm1hLmNvbS9bY19jYW1lcmZpcm1hX2xlZ2Fs X3Bl
cnNvbnMMjAxNi5jcmwwRaBDoEGGP2h0dHA6Ly9jcmwxLmNhbWVyZmlybWEuY29tL2Fj X2NhbWVy
ZmlybWFbGVnYWxfcGVyc29uczQyMDE2LmNvbDBzBgNVHREEbDBkgRphZG1pbmlzdHJhY2lvbkBp
dm5vc3lzLmNvbaRMMEoxSDBGBgorBgEEAYGHLb4KDDhDRVJUSUZJQ0FETyBFTEVDVFJPTklDTyBD
VUFMSUZJQ0FETyBERSBTRUxMTyBFTEVDVFJPTklDTzAcBgNVHRIEFTATgRFjYUBjYW1lcmZpcm1h
LmNvbTCB1AYDVR0gBIHMMIHJMIG7BgtrBgEEAYGHLgoQAgECMIGpMCkGCCsGAQUFBwIBFh1odHRw
czovL3Bvb3ljeS5jYW1lcmZpcm1hLmNvbTB8BggrBgEFBQcCAjBwDGSDZXJ0aWZpY2FkbyBjdWFs
aWZpY2FkbyBkZSBzZWxsbyBlbGVjdHJvbmljbyAgQ29uc3VsdGUgbGFzIGNvbmRpY2lvbmVzIGRl
IHVzbyBlbiBodHRwczovL3BvbGljeS5jYW1lcmZpcm1hLmNvbTAJBgcEAIvsQAEBMIGKBggrBgEF
BQcBAwR+MHwwCAYGBACORgEBMAsGBgQAjkYBAwIBDzBOBgYEAI5GAQUwRDAgFhpodHRwczovL3Bk
cy5jYW1lcmZpcm1hLmNvbKMCRU4wHBYaaHR0cHMvLy9uZHMuY2FtZXJma3RhYS5jb20TAkVTMBMG
BgQAjkYBBjAJBgcEAI5GAQYCMA0GCSqGSIb3DQEBCwUAA4ICAQC0K6l/ohgkE0wPWmyT0kuMFud
/roRBp3BNMnqwNl4F+NGwthQbspn3fj09X4/MoEa1m/YOgspSRZu0kX9QwiWkN/Wd6ypmg0yZVbr
dj+T2/9VkhwIEOrs0W6wNuMD7V94lQyYvvUWgU+iM6zxcVW4Rn9B0kYIIhIx1A4VhbgyewG2uFD
d1uJZIgOoqgVO2b9MTIXcJFw2E+0A0lbddhnRq+EhrW4v6lhFr9O18mphdZlWJj+CDvIZlRzpqq4+
Yro6y97NZHG9K5i6W4Z+dwKCy8MINgcnBjV34S7YAQmMd0mk2mH+XLPW4MMzPFYcqVrnUEDNBoI
Tjdu5z4/V14Lai3uu0bGliL+MKZxogOPlKIJcaP+tBxwJGWp34BVRQcBKiNSkWqtRTE0htAUA0o
nX34dHB7akfK0r8SqBIOl7kPnYIzXJ70qMJP8h6VLjhIov39uVLSlpjwYjIs54v8c6PgrXBZAGgJ
uHrv83nY6DSrctyPL76jmh+nO//McjQLxNNkqJh9Yezhow9N4WNHxtVEeFK7GPv07o4FCoTITgvG
PrmyAmwrBDq6ATE5BBmNlEqkNk6aH5bR117oSiQcThoOFYrc75AtR+25Q2ZVsYM0kwUkFUk/oRtF
Xq0Q4Y8Lkwp16sQi4lOZjgcr7Bs37Yjpnote6KfoFZJNJarV3A==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Issuer OU:	*see current address at https://www.camerfirma.com/address*
Issuer ST:	*MADRID*
Issuer L:	*MADRID*
Issuer C:	*ES*
Subject C:	*ES*
Subject O:	*IVNOSYS SOLUCIONES S.L.U.*
Subject OU:	*GERENCIA*
Subject OU:	*DIRECCION IT*
Subject 2.5.4.97:	*VATES-B98333362*
Subject CN:	*SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS SOLUCIONES*
Valid from:	*Tue Dec 10 17:58:29 CET 2019*
Valid to:	*Sat Dec 09 17:58:29 CET 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:97:98:40:EB:AA:62:7B:0C:BB:AF:77:FD:5D:18:A7:4C:4C:8E:DF:75:B9:F6:00:86:76:A4:01:2E:CE:6C:99:80:2E:E4:14:80:B6:FB:A9:1C:F6:3F:22:22:3F:3A:87:5F:F8:2B:31:B6:6F:32:AC:06:4A:39:51:0A:1B:4D:85:0C:5F:DC:09:5A:FE:90:66:56:4A:02:61:7F:C2:DA:2C:B5:C3:78:45:AF:19:8C:BC:24:CF:39:ED:30:A9:3D:AD:BD:1C:9F:17:D5:6C:A8:02:DC:FB:2C:DD:15:8B:06:80:32:C8:08:BA:6F:5A:2E:D6:61:91:E5:91:27:C6:69:F1:BE:C8:43:0A:A7:A8:6A:11:6C:4B:87:B3:34:DB:92:E3:8E:DD:6E:88:A5:09:2D:BF:EC:A9:08:B1:69:48:8F:4E:D4:4C:69:8E:50:22:07:BC:0F:C7:AA:84:70:68:73:DF:DA:8B:10:D3:6B:A7:09:7A:AA:0B:C1:1B:09:BD:2C:9E:D2:66:F2:B1:5F:92:C6:EB:18:0B:18:08:B1:B9:3D:AD:A2:FF:3E:16:F6:54:12:65:1A:5A:E4:20:64:02:8B:07:65:6A:6B:4E:26:86:C5:1F:A9:29:FC:F4:15:C4:65:6A:79:C2:E4:2F:78:4E:5E:E7:4C:97:AE:10:95:CA:67:C9:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Extended Key Usage	*id_kp_clientAuth*
Subject Key Identifier	*AD:A9:06:A9:AA:80:F5:47:5B:2B:95:6D:4B:71:07:4F:6D:63:1F:91*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt* *http://ocsp.camerfirma.com*
Authority Key Identifier	*C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl* *http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl*
Subject Alternative Name	*administracion@ivnosys.com* *OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO*
Issuer Alternative Name	*ca@camerfirma.com*

Certificate Policies	*Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2* *CPS pointer: https://policy.camerfirma.com* *CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]* *Policy OID: 0.4.0.194112.1.1*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*DB:9B:AF:22:84:63:BA:F4:AD:C8:3D:6A:AA:2E:88:69:2A:AD:0C:D3:A4:B6:C3:CD:27:00:1B:5A:86:AE:DD:AA*

X509SubjectName

Subject C:	*ES*
Subject O:	*IVNOSYS SOLUCIONES S.L.U.*
Subject OU:	*GERENCIA*
Subject OU:	*DIRECCION IT*
Subject 2.5.4.97:	*VATES-B98333362*
Subject CN:	*SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS SOLUCIONES*

X509SKI

X509 SK I	*rakGqaqA9UdbK5VtS3EHT21jH5E=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-10-26T01:00:00Z

30.4 - Service (granted): Qualified electronic time stamps issued by "IvSign Qualified TSA 2021"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified electronic time stamps issued by "IvSign Qualified TSA 2021"*

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por "IvSign Qualified TSA 2021"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *404100734891941768288075753007301544443672661421*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIH7zCCBdegAwIBAgIURsiA75JP2thpSsizqbpPVXx2Da0wDQYJKoZIhvcNAQELBQAwgZIxCzAJ
BgNVBAYTAkVTMREwDwYDVQQIDAbWQUxFTkNJQTEXMBUGA1UECwwOVFJVUTQgU0VSVkIDRVMxGDAW
BgNVBGEMD1ZBVEVTL1U1SODMzMzM2MjEiMCAGA1UECgwZSVZOT1NZUyBTT0xVQ0lPTkVTIFMuTC5V
LjEZMBcGA1UEAwwQSXZTaWduIEdsb2JhbCBDQTAeFw0yMTAzMTAxMDA2MThaFw0yNTAzMDkxMDA2
MTdaMG8xIjAgBgNVBAMMGUI2U2lnbiBRdWFsaW2pZWQgVFNBIDIwMjExGDAWBgNVBGEMD1ZBVEVT
LU1SODMzMzM2MjEiMCAGA1UECgwZSVZOT1NZUyBTT0xVQ0lPTkVTIFMuTC5VLjELMAkGA1UEBhMC
RVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCy6YVyk4cADR+r2xGIqBmOTW3Gh5pt
yNN+id7wUQQUt0lybouPiGbZ0u42HscYjxH+3co0YCLoernvHHeZL VUoxQOuqGqrULN0RR1PM
GH7ovBZIPfhXIny3oZi2ur+uF1Mx/6X6rMyMrPNa1pdJ15p66ds7dgkCE0L vfMLmsO0KmYYVb6ZEP
+NX0Iq7R4zi1Xmxw0/F+cMQtQczqxOkl8wdSsEFLxUEdDCwPJa3x7L Ybtoemcl+ewI82rWmQqpUM
bDy1D02rYASZrszvtlsDZGaX8Qz70vLVtSHyPQGTW/XPigV7YJKEDviVwmZ0OQGtP88zJsEwNPYV
o+HqoJzHAgMBAAGjggNdMIIDWTAMBgNVHRMBAI8EAjAAMB8GA1UdIwQYMBaAFOphW16bH7z4KQz6
xN6Sxd7uMTIzMG0GCCsGAQUFBwEBBGEwXzA5BggrBgEFBQcwAoYtaHR0cDovL2NhLmI2c2lnbi5j
b20vY2VydHMvaXZraWduZ2xvYmFsY2EuY3J0MCIGCCsGAQUFBzABhhZodHRwOi8vb2NzcC5pdnNp
Z24uY29tMIIBQwYDVR0gBIIBOjCCATYwggEyBg0rBgEEAYLxSAMQBggEMIIBHzAmBggrBgEFBQcC
ARYaaHR0cHM6L y9wb2xpY3kuaXZub3NScy5jb20wgfQGCCsGAQUFBwICMIHnIoIkAEMAZQByAHQA
aQBmAGkAYwBbAGQAbwAgAGMAdQBbAGwAaQBmAGkAYwBbAGQAbwAgAGQAZQAgAHMAZQBsAGwAbwAg
AGUAbABlAGMAdAByAPMAbgBpAGMAbwAgAGQAZQAgAFQAUwBBAC4AIABDAG8AbgBzAHUAbAB0AGUA
IABsAGEAcwAgAGMAbwBuAGQAaQBjAGkAbwBuAGUAcwAgAGQAZQAgAHUAcwBvACAAZQBuACAaAB0
AHQAcABzADoALwAvAHAAbwBsAGkAYwB5AC4AaQB2AGHAbwBzAHkAcwAuAGMAbwBtMBYGA1UdIQEB
/wQMMAoGCCsGAQUFBwMIMIGUBggrBgEFBQcBAwSBhzCBhDAIBgYEAI5GAQEwCwYGBACORgEDAgEP
MAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGAjBMBgYEAI5GAQUwQjAUFhlodHRwczovL3Bk
cy5pdnNpZ24uY29tL2VzZ5wJlczAIFhlodHRwczovL3Bkcy5pdnNpZ24uY29tL2VuEwJlbyBnBgNV
HR8EYDBcMC2gK6AphidodHRwOi8vY3lsMS5pdnNpZ24uY29tL2l2c2lnbmdsb2JhbC5jcmwwLaAr
oCmGJ2h0dHA6Ly9jcmwyI.mI2c2lnbi5jb20vaXZraWduZ2xvYmFsLmNybDAdBgNVHQ4EFgQU/9oS
yrYkHIw8UHaZ7D5u6FnK/BgwKwYDVR0QBCQwIoAPMjAyMTAzMTAxMDA2MThagQ8yMDIzMDMxMDEw
MDYxOFowDgYDVR0PAQH/BAQDAgbAMA0GCSqGSIb3DQEBCwUAA4ICAQBqrFDLZFhFBdiDQXCT9V3J
rp34vAfrmrPDhYFnPDp+0L ScKhHyO6KqPLvBHhrtGjTg1NO8NAG6G7ka5VYFj6QazqwHR7lk8TWD
apR/wsO5V0vohrmQlWulqIhlQyj1NBsJhduly4AKtqu++Txk8rbVCwPHjpxkYWYwS7VNKBvrv0L5s
V/DIEamqhlqV3MRINd0IahdkuN/GRUAcrTAIH4ZhrnoPLx00TdI5SNQsKVBe00Cpnd2zsAV3PhXKz
xDeq/Els1olbdFrp3lpnf+BYy4GMnuNn4lEDy+rf5fqq3Mn1Pmr2YZbaTXcuo2hCzIP8K46l+IIk
x5WtHvefb0KocuFSq2sei/sFx6iGuN/S3LhjDDmGmmodjsPu++kWrcPJ2lIAcY399YHDTUkg3dJ
vIEZc7kKX06Ya13Qf9WYB8/pew2atel8Dm3s6Qm8wq1tEjwv9I0Fvsdwq Cyl2Gu08lb6bOpVpwe6
c96KXaO6b0jvFBrQ2D0I09YcrM6d+rQ9fIVutaC VhvRCx2C TaKcGIqIh2MeqD4nXQ7PRdI9UGGfT
Hw+aw78amFC6hlrVbBoqB4UkpSadZMKz2qgI9tXGqeqVIAZfgfP+oZqyO90b6n//bMNb6GRE5qmR
v8gOrtTy8zIXM8xXWgGhwwNMmmCJ18vQC4OnxfxfDstDgpGRIjtvKA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *IvSign Global CA*

Issuer O: *IVNOSYS SOLUCIONES S.L.U.*

Issuer 2.5.4.97: *VATES-B98333362*

Issuer OU: *TRUST SERVICES*

Issuer ST: *VALENCIA*

Issuer C: *ES*

Subject C: *ES*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject CN: *IvSign Qualified TSA 2021*

Valid from: *Wed Mar 10 11:06:18 CET 2021*

Valid to: *Sun Mar 09 11:06:17 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:E9:85:72:93:87:80:0D:1F:AB:DB:11:88:A8:19:8E:4D:6D:C6:87:9A:6D:C8:D3:7E:89:DE:F0:51:04:09:0A:DD:25:C9:BA:2E:3E:21:9B:67:4B:B8:D8:7B:1C:62:3C:47:FB:77:22:D1:80:8B:A1:EA:E6:BC:81:C8:79:92:D5:52:8C:50:39:AA:86:AA:BB:54:2C:DD:11:45:43:CC:18:7E:E8:BC:16:48:3D:F8:57:87:2D:E8:66:2D:AE:FB:01:75:33:1F:FA:5F:AB:6B:33:23:2B:3C:D6:B5:A5:D2:75:E6:9F:FA:EA:1E:DD:AA:40:84:D0:BB:DF:30:B9:AC:3B:42:A6:55:85:5B:F1:91:0F:F8:D5:F4:26:AE:D1:E3:38:B5:5E:6C:70:D3:F1:7E:70:C4:2D:41:CC:EA:C4:E9:25:F3:07:52:B0:41:4B:C5:41:1D:0C:2C:0F:25:AD:F1:EC:B6:1B:B6:87:A6:72:5F:9E:C0:8F:36:AD:69:90:AA:95:0C:6C:3C:B5:0F:4D:AB:60:04:99:AE:CC:EF:B6:5B:03:64:66:97:F1:0C:FB:D2:F2:D5:B5:21:F2:3D:01:93:5B:F5:CF:8A:05:7B:60:92:84:0E:F8:95:C2:66:74:39:01:AD:3F:CF:33:26:C1:30:34:F6:15:A3:E1:EA:A0:9C:C7:02:03:01:00:01

Basic Constraints

IsCA: false

Authority Key Identifier

EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33

Authority Info Access

http://ca.ivsign.com/certs/ivsignglobalca.crt

http://ocsp.ivsign.com

Certificate Policies

Policy OID: 1.3.6.1.4.1.47304.3.16.6.8.4

CPS pointer: https://policy.ivnosys.com

CPS text: [Certificado cualificado de sello electrónico de TSA. Consulte las condiciones de uso en https://policy.ivnosys.com]

Extended Key Usage

id_kp_timeStamping

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

id_etsi_qcs_QcSSCD

CRL Distribution Points

http://crl1.ivsign.com/ivsignglobal.crl

http://crl2.ivsign.com/ivsignglobal.crl

Subject Key Identifier

FF:DA:12:CA:D5:64:1C:9C:3C:50:76:99:EC:3E:6E:E8:5A:4A:FC:18

Key Usage:

digitalSignature - nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

A5:C2:AA:07:A1:59:F4:ED:C9:F5:67:EC:5D:01:BC:D1:46:91:52:30:58:9E:4B:B7:E4:41:08:DA:93:B3:2E:AF

X509SubjectName

Subject C:

ES

Subject O:

IVNOSYS SOLUCIONES S.L.U.

Subject 2.5.4.97:

VATES-B98333362

Subject CN:

IvSign Qualified TSA 2021

X509SKI

X509 SK I

/9oSytVkHJw8UHaZ7D5u6FpK/Bg=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time *2021-10-26T01:00:00Z*

31 - TSP: Logalty Prueba por Interposición, S.L.

.

TSP Name

Name	[en]	*Logalty Prueba por Interposición, S.L.*
Name	[es]	*LOGALTY SERVICIOS DE TERCERO DE CONFIANZA, S.L*

TSP Trade Name

Name	[en]	*Logalty Servicios de Tercero de Confianza SL*
Name	[es]	*Logalty Servicios de Tercero de Confianza SL*
Name	[en]	*VATES-B84492891*
Name	[es]	*VATES-B84492891*
Name	[en]	*Logalty Prueba por Interposicion SL*
Name	[es]	*Logalty Prueba por Interposicion SL*

PostalAddress

Street Address	[en]	*Calle Valportillo Primera, 22, 1ª planta modulo 7 y 8*
Locality	[en]	*Alcobendas*
State Or Province	[en]	*Madrid*
Postal Code	[en]	*28108*
Country Name	[en]	*ES*

ElectronicAddress

URI	[en]	*mailto:info.ca@logalty.com*
URI	[en]	*https://www.logalty.com/en/*
URI	[es]	*https://www.logalty.com*

TSP Information URI

URI	[en]	*https://www.logalty.com/en/*
URI	[es]	*https://www.logalty.com/*

31.1 - Service (granted): Certificados cualificados emitidos por Logalty Qualified CA G2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados cualificados emitidos por Logalty Qualified CA G2*

Name *[en]* *Qualified Certificates issued by Logalty Qualified CA G2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6317076465733621721*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHHzCCBh+gAwIBAgIIV6rDk4cIV9kwDQYJKoZIhvcNAQENBQAwgcfxGDAWBgNVBGEMD1ZBVEVT
LUI4NDQ5Mg5MTEbMBkGA1UEAwwSTG9nYWx0eSBDQSBST09UIDAzMR8wHQYDVQQLDBZMb2dhbHR5
IFRydXN0IFNlcnZpY2VzMTUwMwYDVQQDCxMb2dhbHR5IFNlcnZpY2lvcyBkZSBUZXIjZXJvGRl
IENvbmZpYW56YSBTTDETMBEGA1UEBwwKQWxjb2JlbmRhczEPMA0GA1UECAwGTWFkcmlkMQswCQYD
VQQGEwJFUzAcFw0xODA2MDYxMTA4NDlaFw0zMTA2MDYxMTA4NDlaMIHHMSAwHgYDVQQDDBdMb2dh
bHR5IFF1YWxpZmllZCBDQSBHMjEtMB0GA1UECwwWTG9nYWx0eSBUcnVzdCBTZXJ2aWNlczEYMBYG
A1UEYQwPVkFURVMtQjg0NDkyODkxMTUwMwYDVQQKDCxMb2dhbHR5IFNlcnZpY2lvcyBkZSBUZXJj
ZXJvIGRlIENvbmZpYW56YSBTTDETMBEGA1UEBwwKQWxjb2JlbmRhczEPMA0GA1UECAwGTWFkcmlk
MQswCQYDVQQGEwJFUzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANFRdb/bH/xTJjR9
u8Iy4+8tCjYw5yMBg4MXne7TypdnhspatIeXdXn5OEzxqu6yzWCKWy0RSCoL8pTiB+MgZWWzPp
J1utcunHe5YwwCBYM65+SQ8zd2YaSzzLvyYuujIIuYXX6ewexuHbmzGmN52zBGEkuZHBgUZoce8
KsH6XNk16KsuTmH5XXdvd83Im7dsVvCj06Lw2BXauNE2YBDZU1BLRZ5fD9Nz0KzY6tgKTcXrfLXx
EDRpCIVch8D99IQesVStQeT+5I0dHpp1mnvzF9Bql8vLx4ZsJvcq5J/HGYO5KG80NdsoCgS1pZibl
A6vtrZ6SKfmSlERlhU+ily14E3QO+fc/2SJ7d0CEKE315uAAq1IyZSkTMCVGfv6t12SRF1gYAX4/
PvUyGHu2Dc1RdercPgy5GbMrI4Sr8ionH4anWFwRM44aVUWdZyb9L1j/N+T1/BVLAKuH2KwmGFA9
z3nhlSLApWTxgmic/faDUE94shfZDBzX1kmUC1Sp72IzpYsVwyAVMHtqSoXQ8YmMybEQ5rRer
PLzwTP5yzEn9MWc1tFRRO/d16S/pxuoJMxh34byHfvM9VLya9FMaBjRb6oGjPk2vELQhHbFi8AIj
JDveGDKAjc6jQCrEFy6ujDzQZsMkim+XM9bS94iTmkVy9ecxhJgfIB7JduxAgMBAAGjggHIMIIB
xDASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFHsxTarAqI4r4+2tiBQISYzGqi6CMIGi
BggrBgEFBQcBAQSBfTCBkjBSBggrBgEFBQcwAoZGaHR0cHM6Lzk93dXcubG9nYWxlcS5lcy9jZXI0
aWZpY2F0ZWF1dGhvcml0cS9Mb2dhbHR5Q0FST09UMDMuY2FjZXJ0LmNydDABBggrBgEFBQcwAYYw
aHR0cDovL29jc3AxLmxvZ2FsdHkuZXM7IGh0dHA6Ly9vY3NwMi5sb2dhbHR5LmVzMEoGA1UdIARD
MEEwPwYEVR0gADA3MDUGCCsGAQUFBwIBFilodHRwczovL3d3dy5sb2dhbHR5LmVzL1BLSS9kh2N1
bWVudGFjaW9uLzBtBgNVHR8EZjBkMDCgLqAshipodHRwOi8vY3JsMS5sb2dhbHR5LmVzL2xvZ2Fs
dHlDQVJvb3QwMy5jcmwwMKAuoCyGKmh0dHA6Ly9jcmwyLmxvZ2FsdHkuZXMvbG9nYWx0eUNBUm9v
dDAzLmNybDAdBgNVHQ4EFgQUkk+pa/3ZUk6lChXW+E6OKNS4mwwDgYDVR0PAQH/BAQDAgEGMA0G
CSqGSIb3DQEBDQUAA4ICAQBCA6tyAKMh0TubLbeq+P9F1W8xuFCPvuf+aSMkOmwrS/DshuilUbWu
Zpncw3cuk1pbTqsmPo17rGcvE5XvLmesws/bdU4/7zeCzzAu1sePmMU1V+hSraKiPA2IazG7Dc
m/MPCM+OuA/obbtU/tkyYk12qO9jeEPA4BPUpdw+Ypz5Ov3cwdVWgNR5mu1lm7BJ+xvCr+NRbkX7T
HRBuZ2MjbVBSHEPFb80Yu+aqYOj5p0dFK5wrqTJ0a4cU8VQuTyvYmMK00UscMGhXxnO3KhxEQjcw
WQFSPt9Bx11LvHVRNT0R4qHB7+2xh0rUdK9p0CW39D2M97KZvpIgn7+hr3RhrtwVjDb9qfVzE2
Vxad2ysHbr0KVIdJgZC6ffp55c8eIQnI2Em6TJ0kGZcVL198JC+7p+cfGjmPwQ/yyrE6E
RYxcZP1u3mARTu4JOfC3gvUDSbVh1rqpOybvEmfUlE6NeFT5HRcxWqJexgSoECqPPVeJEgtkq
IOReM6DKYY2dreaCEPVxzMnnPjEaNKmFt23pxwd/dcjFK5daHyBOHRxJC1FF72vv7GdeGtVZA2Eb
skpzeopUFN6e/Z2kcyEN5UcMdvjM9p+++HgoQhiiUyFJ9Vbah8NS5mM3VKr1YGeLDDzXsqy3O/rz
b74H52P918I7gRis86zzag==

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *Madrid*

Issuer L: *Alcobendas*

Issuer O: *Logalty Servicios de Tercero de Confianza SL*

Issuer OU: *Logalty Trust Services*

Issuer CN: *Logalty CA ROOT 03*

Issuer 2.5.4.97: *VATES-B84492891*

Subject C:	*ES*
Subject ST:	*Madrid*
Subject L:	*Alcobendas*
Subject O:	*Logalty Servicios de Tercero de Confianza SL*
Subject 2.5.4.97:	*VATES-B84492891*
Subject OU:	*Logalty Trust Services*
Subject CN:	*Logalty Qualified CA G2*
Valid from:	*Wed Jun 06 13:08:49 CEST 2018*
Valid to:	*Fri Jun 06 13:08:49 CEST 2031*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:51:75:BF:DB:1F:FC:53:26:34:7D:BB:C9:72:8B:8F:BC:B4:28:D8:C3:9C:8C:06:0E:0C:5E:77:BB:4E:FA:5D:9E:1B:29:6A:D2:1E:5D:D5:E7:E4:E1:33:C6:AB:BA:CB:35:82:29:6C:B4:45:20:A8:2F:CA:53:B4:1F:8C:81:95:96:89:9A:4F:27:5B:AD:72:E9:C7:7B:96:30:C0:20:58:33:AE:7E:49:06:DD:D9:8B:92:CE:C7:CB:BF:26:2E:BA:37:E5:8A:26:17:5F:A7:B0:7B:1B:87:6E:67:86:98:DE:76:C5:11:84:92:E6:47:F2:05:19:A1:EC:FC:2A:C1:FA:5C:D9:35:E8:AB:2E:4E:61:F9:5D:77:6F:77:CD:DF:9B:B7:6C:56:F0:A3:27:A2:F0:D8:15:DA:B8:D1:36:60:10:D9:53:50:4B:45:9E:5F:0F:D3:73:D0:AC:D8:EA:D8:0A:4D:C5:EB:7C:B5:F1:10:34:69:08:85:5C:87:C0:FD:21:07:AC:55:2B:50:79:3F:B9:23:47:47:A6:9D:66:9E:FC:C5:F4:1A:88:F2:F2:F1:E1:9B:09:BD:EA:B9:27:F1:C6:60:EE:4A:1B:CD:0D:76:CA:02:81:2D:69:66:26:E5:03:AB:EB:AD:9E:92:29:F9:92:94:44:48:85:4F:A2:23:2D:78:13:74:0E:F9:F7:3F:D9:22:7B:77:40:84:28:4D:F5:E6:E0:00:AB:59:72:67:99:13:30:25:46:7E:FE:AD:D7:64:91:17:58:18:01:7E:3F:3E:F5:32:18:7B:B6:0D:CD:51:75:EA:DC:3E:0C:B9:19:B3:2B:D7:84:AB:F2:89:C8:E1:A9:D6:17:04:4C:E3:86:95:51:62:5D:67:26:FD:2C:88:FF:37:F4:C9:FC:15:4B:00:AB:87:D8:AC:26:18:50:3D:CF:79:E1:95:22:C0:A5:64:F1:82:78:9C:FE:37:DA:0D:41:3D:E2:C8:5F:64:30:73:5F:59:26:50:2D:52:A7:FE:F6:23:3A:58:B1:5C:32:01:53:07:AE:A4:A8:5D:0F:18:98:CF:F2:6C:44:39:AD:17:AB:3C:BC:F0:4C:FE:72:CC:49:FD:31:67:35:88:54:51:3B:F7:75:E9:2F:E9:C6:EA:09:33:18:77:E1:BC:87:7E:F3:3D:54:BC:9A:F4:53:1A:06:34:5B:EA:81:A3:3E:4D:AF:10:B4:21:1D:B1:62:F0:02:23:24:3B:DE:18:32:80:8D:EE:A3:40:2A:C4:17:2E:AE:8C:3C:D0:66:C3:24:8A:6F:97:33:D6:D2:F7:88:93:9A:45:72:F5:E7:B1:84:98:1F:B4:1E:C9:76:EB:B1:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*7B:31:4D:AA:C0:A8:8E:2B:E3:ED:AD:88:14:08:49:8C:C6:AA:2E:82*
Authority Info Access	*https://www.logalty.es/certificateauthority/LogaltyCAROOT03.cacert.crt* *http://ocsp1.logalty.es; http://ocsp2.logalty.es*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.logalty.es/PKI/documentacion/*
CRL Distribution Points	*http://crl1.logalty.es/logaltyCARoot03.crl* *http://crl2.logalty.es/logaltyCARoot03.crl*
Subject Key Identifier	*26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*05:95:C5:69:7A:6A:90:AE:41:15:6F:BF:8A:79:52:40:F9:54:B6:4D:77:61:8A:AC:81:2A:55:62:3E:9A:13:6F*

Certificate fields details

Version:	*3*
Serial Number:	*2682646734725033920*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHuzCCBaOgAwIBAgIIJTqs/fElr8AwDQYJKoZIhvcNAQENBQAwgcIxGDAWBgNVBGEMD1ZBVEVT
LUI4NDQ5MjgfMTEbMBkGA1UEAwwSTGQ9aYWx0eSBDQSBST09fIDAzMR8wHQYDVQQLDBZMb2dhbHR5
IFRydXN0IFNlcnZpY2VzMTUwMwYDVQQKDCxMb2dhbHR5IFNlcnZpY2lvcyBkZSBUZXJjZCIvIGRl
IENvbmZpYW56YSBTTDETMBEGA1UEBwwKQWxjb2llbmRhczEPMA0GA1UECAwGTWFkcmlkMQswCQYD
VQQGEwJFUzAeFw0yMDA5MDQxMjA3MThaFw0zMzA5MDQxMjA3MThaMIHHMSAwHgYDVQQDDBdMb2dh
bHR5IFF1YWxpZmllZCBDQSBBMjEiMB0GA1UECwwWTG9nYWx0eSBlUcnVzdCBTZXJ2aWNlczEYMBYG
A1UEYQwPVkFURVMtQjg0ODkxMTUwMwYDVQQKDCxMb2dhbHR5IFNlcnZpY2lvcyBkZSBUZXJj
ZXJvIGRlIENvbmZpYW56YSBTTDETMBEGA1UEBwwKQWxjb2llbmRhczEPMA0GA1UECAwGTWFkcmlk
MQswCQYDVQQGEwJFUzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANFRdb/bH/xTfjR9
u8Iy4+8tCJYw5yMHg4MXne7TvpdnhspatIeXdXn5OEzxqu6yzWCKWy0RSCoL8pI1B+MgZWWzPP
J1utcumHe5YwwCBYM6t5+SQbd2YaSzeILvyYuujIIiYXX6ewxuHbmeGmN52x8GEkuZHKgUZocz8
KsH6XNk16KsuTmH5XXdvd83fm7dsVvCj36L w2BXauNE2YBDZU1BLRZ5fD9Nz0KzY6tgK TcXrfLXx
EDRpCIVch8D9IQesVStQeT+5I0dHpp1mnvzF9Bql8vLx4ZsJvcq5J/HGYO5KG80NdsoCgS1pZibl
A6vrrZ6SKfmSlERlbU+ily14E3QO+fc/2SJ7d0CEKE315uAaq1IyZ5kTMCVGfv6t12SRF1gYAX4/
Pv1yGHu2Dc1RdercPgy5GbMrT4Sr8onH4anWFwRM44aVUWddZyb9LJ/N+TJBVLAKuFI2KwrmGFA9
z3nhlSLApWTxgnic/jfaDUE94shfZDBzX1kmUC1Sp/72lzpYsVwyAVMHqSoXQ8YmM/ybEQ5rRer
PLzwTP5yzEn9MWc1iFRRO/d16S/pxuoJMxh34byHfvM9VLya9FMaBjRb6oGjPk2vELQhHbFi8Alj
JDvcGDKAje6jQCrEFy6ujDzQZsMkzm+XM9bS94iTmkVy9ezxhJgfIB7dduxAgMBAAGjggGsMIIB
qDASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFHxxTarAqI4n4+2tiBQISYzGqt6CMIGG
BggrBgEFBQcBAQR6MHgwUQYIKwYBBQUHMAKGRWh0dHA6Ly9jcnQubG9nYWx0eS5lcy9jZXJ0aWZp
Y2F0ZWF1dGlhvcml0eS9Mb2dhbHR5Q0FST09UMDMuY2FjZXJ0LmNydDAjBggrBgEFBQcwAYYXaHR0
cDovL29jc3AxLmxvZ2FsdHkuZXMwSgYDVR0gBEMwQTA/BgRVHSAAMDcwNQYIKwYBBQUHAgEWKWh0
dHBzOi8vd3d3LmxvZ2FsdHkuZXMvU1EtUL2RyY3VtZW50YWNpb24vMG0GA1UdHwRmMGQwMKAuoCyG
KmhtdHA6Ly9jcmwxLmxvZ2FsdHkuZXMvbG9nYWx0eUNBUm9vdDAzLmNvbDAwoC6gLIYqaHR0cDov
L2NybDIubG9nYWx0eS5lcy9sb2dhbHR5Q0FSb290MDMuY3JsMB0GA1UdDgQWBBQmST6lr/dlSTqU
KFdb4Rs4o1LibDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQENBQADggIBAFfhnOct7Mp2I2SB
KPfDEoA5QtrNf7JNz3W7brxweR5u6jf1Ns/6iZ4U476ZB4wLthbH5i/6ZT3dL NrPocVgfUVYaV9A
KFSI+du1MxcbqHBRxqhPjC2P6FdLVe0lKNr4aydF7qp2lbHKB5wr6NSq5mbgyKSZ72wLuU4PMeg
wUGv+8EsUGEfgCBBK37Xy5N0IKxQLzPFPnYhjrFcFVvfkOnGnhD3w/C67Zc/jHF5dRzU6VNNB2sG
zuCEAe55KpQgz4d63S4HR0Y8aros0fPNbaL+zMJyKZyzwZFwoZgrIKBwU16ABr3S0Y2SSdEFMeXE
YzrOMeU3uJafd7/2XEF80qD7IV6svwIZSMbEqtGr1CKh3GTNTLLbIS+6XIU1+wv+kAhxK1sEGF3
OzX3R2p8gvUaQMew10bb+aQzpk+QsjmEj1RvExOOlG5RkobTzWrQUV49X6QOiEw7yaS1ofXPcX
oV47DzM687OoxqzTMlt+H1oAVHuH+Iub9lEOQdOaj5iX+lkD1u7RDgGZuFU9L81io/Cv0aGDq0kT
joSLKoFZ9PQB8qs4l0mHoSL2hf2cBchhprT+RjpcLBbM4PXYPtb2/RhmtbL25hHOz9Pmgjd+hh3a
ocDcuaaWLANKqKngTZSUlaBeNaz3vqtji1n8H4Duk3SxOPIGHafjlyqtCEyW

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *Madrid*

Issuer L: *Alcobendas*

Issuer O: *Logalty Servicios de Tercero de Confianza SL*

Issuer OU: *Logalty Trust Services*

Issuer CN: *Logalty CA ROOT 03*

Issuer 2.5.4.97: *VATES-B84492891*

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified CA G2*

Valid from: *Fri Sep 04 14:07:18 CEST 2020*

Valid to: *Sun Sep 04 14:07:18 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:51:75:BF:DB:1F:FC:53:26:34:7D:BB:C9:72:8B:8F:BC:B4:28:D8:C3:9C:8C:06:0E:0C:5E:77:BB:4E:FA:5D:9E:1
B:29:6A:D2:1E:5D:D5:E7:E4:E1:33:C6:AB:BA:CB:35:82:29:6C:B4:45:20:A8:2F:CA:53:B4:1F:8C:81:95:96:89:9A:4F:27:5B:AD:72:E9:C7:7B:96:30:C0:20:58:33:AE:7E:49:06:DD:D9:8B:92:CE:C7:CB:BF:26:2E:BA:37:E5:
8A:26:17:5F:A7:B0:7B:1B:87:6E:67:86:98:1E:76:C5:11:84:92:E6:47:F2:05:19:A1:EC:FC:2A:C1:FA:5C:D9:35:E8:AB:2E:4E:61:F9:5D:77:6E:77:CD:DF:9B:B7:6C:56:F0:A3:27:A2:F0:D8:15:DA:B8:D1:36:60:10:D9:53:50:4
B:45:9E:5F:0F:D3:73:D0:AC:D8:EA:D8:0A:4D:CS:EB:7C:B5:F1:10:34:69:08:85:5C:87:C0:FD:21:07:AC:55:2B:50:79:3F:B9:23:47:47:A6:9D:66:9E:FC:C5:F4:1A:88:F2:F2:F1:E1:9B:09:BD:EA:B9:27:F1:C6:60:EE:4A:1B:
CD:0D:76:CA:02:81:2D:69:66:26:E5:03:AB:EB:AD:9E:92:29:F9:92:94:44:48:85:4F:A2:23:2D:78:13:74:0E:F9:F7:3F:D9:22:7B:77:40:84:28:4D:F5:E6:E0:00:AB:59:72:67:99:13:30:25:46:7E:FE:AD:D7:64:91:17:58:18:01:7E
:3F:3E:F5:32:18:7B:B6:0D:CD:51:75:EA:DC:3E:0C:B9:19:B3:2B:D7:84:AB:F2:89:C8:E1:A9:D6:17:04:4C:E3:86:95:51:62:5D:67:26:FD:2C:88:FF:37:E4:C9:FC:15:4B:00:AB:87:D8:AC:26:18:50:3D:CF:79:E1:95:22:C0:A5:
64:F1:82:78:9C:FE:37:DA:0D:41:3D:E2:C8:5F:64:30:73:5F:59:26:50:2D:52:A7:EE:16:23:3A:58:B1:5C:32:01:53:07:AE:A4:A8:5D:0F:18:98:CF:F2:6C:44:39:AD:17:AB:3C:BC:F0:4C:1E:72:CC:49:FD:31:67:35:88:54:51:3B
:F7:75:E9:2F:E9:C6:EA:09:33:18:77:E1:BC:87:7E:F3:3D:54:BC:9A:F4:53:1A:06:34:5B:EA:81:A3:3E:4D:AF:10:B4:21:1D:B1:62:F0:02:23:24:3B:DE:18:32:80:8D:EE:A3:40:2A:C4:17:2E:AE:8C:3C:D0:66:C3:24:8A:6F:97:
33:D6:D2:F7:88:93:9A:45:72:F5:E7:B1:84:98:1F:B4:1E:C9:76:EB:B1:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier	*7B:31:4D:AA:C0:A8:8E:2B:E3:ED:AD:88:14:08:49:8C:C6:AA:2E:82*
Authority Info Access	*http://crt.logalty.es/certificateauthority/LogaltyCAROOT03.cacert.crt* *http://ocsp1.logalty.es*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.logalty.es/PKI/documentacion/*
CRL Distribution Points	*http://crl1.logalty.es/logaltyCARoot03.crl* *http://crl2.logalty.es/logaltyCARoot03.crl*
Subject Key Identifier	*26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C0:70:69:EB:4A:AE:CF:16:0B:7D:EC:65:52:69:5F:28:8F:8D:75:2B:DA:C9:2B:E2:0B:C6:C1:C3:F6:C5:7A:C8*

X509SubjectName

Subject C:	*ES*
Subject ST:	*Madrid*
Subject L:	*Alcobendas*
Subject O:	*Logalty Servicios de Tercero de Confianza SL*
Subject 2.5.4.97:	*VATES-B84492891*
Subject OU:	*Logalty Trust Services*
Subject CN:	*Logalty Qualified CA G2*

X509SKI

X509 SK I	*Jkk+pa/3ZUk6lChXW+EbOKNS4mw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-10-28T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI [es] *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

31.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

31.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

31.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

31.1.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.30210.1.1.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.30210.1.2.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.30210.1.6.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.30210.1.7.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.30210.1.3.1*

Description

31.1.5 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[es]*	*Certificados cualificados emitidos por Logalty Qualified CA G2*
Name	*[en]*	*Qualified Certificates issued by Logalty Qualified CA G2*

Service digital identities

X509SubjectName

Subject C:	*ES*
Subject ST:	*Madrid*
Subject L:	*Alcobendas*
Subject O:	*Logalty Servicios de Tercero de Confianza SL*
Subject 2.5.4.97:	*VATES-B84492891*
Subject OU:	*Logalty Trust Services*
Subject CN:	*Logalty Qualified CA G2*

X509SKI

X509 SK I *Jkk+pa/3ZUk6lChXW+EbOKNS4mw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-11-28T01:00:00Z*

31.1.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

31.1.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

31.1.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

31.1.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.6.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.7.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.3.1

Description

31.2 - Service (granted): Sellos de tiempo cualificados emitidos por Logalty Qualified TSA TSU005

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.

[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name *[es]* *Sellos de tiempo cualificados emitidos por Logalty Qualified TSA TSU005*

Name *[en]* *Qualified timestamps issued by Logalty Qualified TSA TSU005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2600299901454462975*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJyDCCB7CgAwIBAgIIJBYc+7+tL/8wDQYJKoZIhvcNAQENBQAwgccxIDAeBgNVBAMMF0xvZ2Fs
dHkgUXVhbGlmaWVkIENBIEcyMR8wHQYDVQQLDBZMb2dhbHR5IFRydXN0IFNlcnZpY2VzMRgwFgYD
VQRhDA9WQVRFUy1CODQ0OTI4OTExNTAzBgNVBAoMLExvZ2FsdHkgU2VydmljaW9zIGRlIFRlcmNl
cm8gZGUgQ29uZmllbnphIFNMMRMwEQYDVQQHDApBbGNvYmVuZGFzMQ8wDQYDVQQIDAZNYWRyaWQx
CzAJBgNVBAYTAkVTMB4XDTE4MTAyMzE2MzIyMFoXDTIzMTAyMjE2MzIyMFowgaExTTAjBgNVBAMM
HExvZ2FsdHkgUXVhbGlmaWVkIFRTQSBUU1UwMDUxHzAdBgNVBAsMFkxvZ2FsdHkgVHJ1c3QgU2Vy
dmljZXMxNTAzBgNVBAoMLExvZ2FsdHkgU2VydmljaW9zIGRlIFRlcmNlcm8gZGUgQ29uZmllbnph
IFNMMRMwEQYDVQQHDApBbGNvYmVuZGFzMQswCQYDVQQGEwJFUzCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBAJTrkc9tO6Kx1MCxCbVXPQrnVozWYtYaswddp9ZsbuLXBcjfjnwoNvyJmU/A4
wZeoZ2NqWFOxz07FV+gtVHfc7Wv8lxLfY+vCdPSuLH5nTON+pEYM/IlwaTnPMBv2t3+j4OFG0EId
xt4VH7wlZApfOQz1cKduoXmkAwKYbAdbIl31hoDjxbggHr2q8BPSYYhpcR8VT6gAdKtS+ny/J5n4
n4RDovBPN8mMimoebbKON5pbWhcCf+TvdLdYbjKIMu4PBG1jlD416R8jVQlWpH16VKqnLrGGQ+rN
bR4YzNHWPtx7umE/loXcMgtL YvFxbmh6IFP61W0SNcA93jqQHZAbOWineWdLbMzbHJgGy8HGR7EI
rq+VtKH6jmyLthpHEdJuaD1WISNoU2fiE7PFs9N9pmz6/C0Ab2kTEgff0g639C1b2TeBdyaH4DVd
Nz6Z9L3EADmSOTpKP/9fSlXPUrURZ6Kmrg9NeDNAuNw5BPy21KdoyFni+qOJ7GHJMEejXQoAj/X
/V0WUNJkmSclh+u1rU1rTPy5i7aefNx5Z6ENvN4U84g+sNfybURV3XFPBcXoDucjY7wjm10ozjy
MVPvSQC9uBkMc8c5e0hMYNnYDc5HzD5ymkgaDh+tPbk6+wpbZ5NJyc2U9tmP03CyzxbDiVxIM
fBSR19rjxw12k81zAgMBAAGjggPaMIID1jCBbQYIKwYBBQUHAQEEcTB3MFAGCCsGAQUFBzAChkRo
dHRwczovL3d3dy5sb2dhbHR5LmVzL2NlcnRpZmljYXRlYXV0aG9yaXR5L0xvZ2FsdHlRdWFsaWZp
ZWRDQUcyLmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AxLmxvZ2FsdHkuZXMwHQYDVR0OBBYE
FOJDw1FTRqAyRzUl8MUw9Kz9p1aceMB8GA1UdIwQYMBaAFCZJPqWv92YJOpQoV1vbGrzjUu3MIHg
BggrBgEFBQcBAwSB0zCB0DAIBgYEAI5GAQEwCwYGBACORgEDAgEPMBMGBgQAjkYBBjAJBgcEAISG
AQYCMIGhBgYEAI5GAQUwgZYwSRZDaHR0cHM6L y93d3cubG9nYWx0eS5lcy9jZXJ0aWZpY2F0ZWF1
dGhvcm0eS9lbi9MR1RfUERTX1RTQS52MXIwLnBkZhMCZW4wSRZDaHR0cHM6Ly93d3cubG9nYWx0
eS5lcy9jZXJ0aWZpY2F0ZWF1dGhvcm0eS9lcy9MR1RfUERTX1RTQS52MXIwLnBkZhMCZXMwggGA
BgNVHSAEggF3MIIBczAJBgcEAIvsQAEBMIIBZAYLKwYBBAGB7AIBBQEwggFTMDMGCCsGAQUFBwIB
F9odHRwczovL3d3dy5sb2dhbHR5LmVzL2NlcnRpZmljYXRlYXV0aG9yaXR5L0NQUzCCARIGCCsG
AQUFBwICMIIBBB6CAQAAQwBlAHIAdABpAGYAaQBjAGEAZABvACAAYwB1AGEAbABpAGYAaQBjAGEA
ZABvACAAZABlACAAcwBlAGwAbABvACAAZQBsAGUAYwB0AHIAswBuAGkAYwBvACAAZABlACAAcABl
AHIAcwBvAGAAYQAgAGoAQB9AOBAZABpAGMAYQAgAHAAYQBvAGEAIABsAGEAIABlAHgAcABlAGQA
aQBjAGkA8wBuACAAZABlACAAcwBlAGwAbABvAHMAIABjAHUAYQBsAGkAZgBpAGMAYQBkAG8AcwAg
AGQAZQAgAHQAaQBlAG0AcABvACAAZQBsAGUAYwB0AHIA8wBuAGkAYwBvMH0GA1UdHwR2MHQwOKA2
oDSGMmh0dHA6Ly9jcmwxLmxvZ2FsdHkuZXMvcXVhbGlmaWVkTG9nYWx0eVN1YkNBMDIuY3JsMDig
NqAOhjJodHRwOi8vY3JsMi5sb2dhbHR5LmVzL.5F1YWxpZmlfZExvZ2FsdHJfdW/IDQTAyLmNybDAO
BgNVHQ8BAf8EBAMCB4AwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwDQYJKoZIhvcNAQENBQADggIB
AE4vgAEN1ySxZvubXcpdMi03Fx/4uvbDTkHbiisztoHEAonAIQoMMhu/9HADlTw0X3ObP8U+/LX
DaGRZCQI17nNPaUvbb0y4x86OCphafoKa1ywL56wsVLGOyj1Lsx5F1FBObrjsqCCQ7Rht6ccVKGV
koav/YgJfAHIbBmxX+9yamuclun5Eoh5WQd3Lc4xqfmHVTQJQRwHO9B9D3ZYTD9Frn5cEiaP6Nq
CBxw1KeL5nCbY/jjE5xtYZeMr4yMislWvu8ihSSW490OsruHihIEk2Plqxycp BZxZ7uKXUrogcWj
oJhulk3X+81jA2Ge6PF9Tq3fsjkQT0PoZlNsdwU+1b1G7H/xox/BoqyV1YrPH8tIQFdJEpGMSAPR
88DUZip/b/B+iCmlEjAW4cJR3MPiKqVhzERuzyugrVvmtQFp3PpjamlORatNlgLSLvYDB1e1bPAJ
TCTXnN07ZZFwPZNSsa2gPlPNzJ9Ng0LehI8ySXFEJn2JMmt4uPTN67/cl+lBw1P0ZaPc/P6Kvss/
tIsTbgMINrocte+8ZKF5uw7R9NPP7AxblyWXlsZCu+AjeRxtL95H/Dvw4dIDbZCm2CbZ5wK4ds0yQ
961xKQ5/zubggJsZiSXE+67ipThMcXN3NosiHbA5Kb/F9AOXuJrH4D0CP9cCuDoiesC+QxaNCmg1

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *Madrid*

Issuer L: *Alcobendas*

Issuer O: *Logalty Servicios de Tercero de Confianza SL*

Issuer 2.5.4.97: *VATES-B84492891*

Issuer OU: *Logalty Trust Services*

Issuer CN: *Logalty Qualified CA G2*

Subject C: *ES*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU005*

Valid from: *Tue Oct 23 18:32:20 CEST 2018*

Valid to: *Sun Oct 22 18:32:20 CEST 2023*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:94:EB:91:CF:4E:E8:AC:75:30:2C:42:85:55:CF:42:2A:E7:56:8C:D6:56:D6:1A:B3:07:5D:A7:D6:6C:6E:E2:D7:05:C8:DF:8E:7C:28:36:F8:C9:99:40:38:C1:97:A8:67:63:6A:58:53:B1:CF:4E:C5:57:E8:2D:54:77:DC:ED:6B:FC:97:12:DF:63:EB:C2:74:F4:AE:2C:7E:67:4C:E3:7E:A4:46:0C:FE:52:30:69:39:CF:30:1B:F6:B7:7F:A3:E0:E1:46:D0:42:1D:C6:DE:15:1F:BC:25:64:0A:5F:39:0C:F5:70:A7:6E:A1:79:A4:03:02:98:6C:07:5B:20:8D:F5:86:80:E3:C5:B8:20:1E:BD:AA:F0:13:D2:61:88:69:79:1F:15:4F:A8:00:74:AB:52:FA:7C:BF:27:99:F8:9F:84:43:A2:F0:4F:37:C9:8C:8A:6A:1E:6D:B2:8E:37:9A:5B:5A:17:02:7F:E4:EF:74:B7:58:6E:32:88:32:EE:0F:04:6D:63:94:3E:35:E9:1F:23:55:09:56:A4:72:3A:54:AA:A7:2E:B1:86:43:E7:CD:6D:1E:18:CC:D1:D6:3E:8C:7B:BA:61:3F:96:85:DC:320B:4B:62:F1:71:6E:68:7A:24:53:FA:D5:6D:12:35:C0:3D:DE:3B:90:1D:90:1B:39:69:DE:59:DF:CB:84:CC:DB:1C:98:06:CB:C1:C6:47:B1:08:AE:AF:95:B4:A1:FA:8E:6C:8B:B6:1A:47:11:D2:6E:68:34:D6:95:23:68:53:67:E2:13:B3:C5:B3:D3:7D:A6:6C:FA:FC:2D:00:6F:69:13:12:07:DF:D2:0E:B7:F4:2D:61:D9:37:01:77:26:87:E0:35:5D:37:3E:99:F4:BD:C4:00:39:92:39:3A:4A:3F:FF:5F:48:85:CF:52:B5:11:67:A2:A6:AE:0F:4D:78:33:40:02:E3:70:E4:13:F2:DB:52:9D:A3:21:67:8B:EA:8E:27:B1:87:24:C1:1E:8D:74:28:02:3F:D7:FD:5D:16:50:D2:64:99:27:25:87:EB:93:AD:44:EB:4C:FC:B9:8B:B6:9E:14:DC:79:67:A1:0D:BC:DE:14:F3:88:3E:B0:D7:F2:85:44:55:DD:71:4F:05:C5:E8:0E:E7:23:63:BC:23:AE:7D:74:A3:38:F2:31:53:EF:49:00:BD:B8:19:0C:73:CB:3F:E5:ED:21:31:83:67:60:37:39:1F:30:F9:CA:69:20:68:E8:7E:70:FB:24:EB:EC:29:85:9B:79:34:DD:72:73:65:3D:B6:63:F4:DC:2C:B3:C6:10:DA:57:12:0C:7C:14:91:23:DA:E3:C7:09:76:93:CD:73:02:03:01:00:01

Authority Info Access

https://www.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt

http://ocsp1.logalty.es

Subject Key Identifier *E2:43:C3:51:53:46:A0:32:47:35:3C:30:9C:3D:2B:3F:69:D5:A7:9E*

Authority Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

Certificate Policies

Policy OID: 0.4.0.194112.1.1

Policy OID: 1.3.6.1.4.1.30210.1.5.1

CPS pointer: https://www.logalty.es/certificateauthority/CPS

CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]

CRL Distribution Points

http://crl1.logalty.es/qualifiedLogaltySubCA02.crl

http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8D:6F:1A:8B:DC:60:5B:88:10:DC:3F:F5:C0:A3:7C:A8:4A:ED:E7:13:DF:9D:87:82:E0:F7:3F:80:8D:82:F0:BA*

X509SubjectName

Subject C: *ES*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU005*

X509SKI

X509 SK I *4kPDUVNGoDJHNTwwnD0rP2nVp54=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-11-28T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

31.3 - Service (granted): Servicio cualificado de entrega electrónica certificada

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description

[en] *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name *[es]* *Servicio cualificado de entrega electrónica certificada*

Name *[en]* *Qualified electronic registered delivery service*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2468400032836762193*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIII/jCCBuagAwIBAgIIkGEwHDMOlEwDQYJKoZIhvcNAQELBQAwgccxIDAeBgNVBAMMF0xvZ2Fs
dHkgUXVhbGlmaWVkIENBIEcyMR8wHQYDVQQLDBZMb2dhbHR5IFRydXN0IFNlcnZpY2VzMRgwFgYD
VQRhDA9WQVRFUy1CODQ0OTI4OTExNTAzBgNVBAoMLExvZ2FsdHkgU2VydmljaW9zIGRlIFRlcmNl
cm8gZGUgQ29uZmlibnphIFNMMRMwEQYDVQQHDApBbGNvYmVuZGFzMQ8wDQYDVQQIDAZNYWRyaWQx
CzAJBgNVBAYTAkVTMBMXDTIzMDIxMjA5MDg0OFoXDTIxMDkxMTA5MDg0OFowgfMcSTBHBgNVBAMM
QFNlbGxvIGRlIGVudHJlZ2EgZWxlY3Ryw7NuaWNhIGNlcnRpZmlyYWRhIGN1YWxpZmlyYWRhIGRl
IExvZ2FsdHkxEjAQBgNVBAUTCU14NDQ5Mjg5MTEtMB0GA1UECwwWTG9nYWx0eSBUcnVzdCBTZXJ2
aWNlczEYMBYGA1UEYOwPVkFURVMtQjg0NDkyODkxMTUwMwYDVQQKDCxMb2dhbHR5IFNlcnZpY2lv
cyBkZSBUZXJjZXIvIGRlIENvbmZpYW56YSBTTDETMBEGA1UEBwwKQWxjb2JlbmRhczEL MAkGA1UE
BhMCRVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCV/zd7fizZcNkQ6r2q0bLgbw5/
14dH4PDMNdltn6Tk1Z6FrUWtYbTxgx4Gtqm15qtj5q3LgWKVg0J+hJldjlAiW2TH4R2KtvBX0pH
wrwI+YczrDcaPxxB74qH7uxkcbAyQMjCNCLQtjX2v829ngfrXYzEMnWt+19cOs0I8aajU8/l0XUm
2pgB2W+j2qnFUAiVjwwngB7RtuuZis0L Dn4z8zdynpFqhZczmHXSDcT32CVYQTau2m0ZuZV2y3DT
5sxMtmbKEcNttrC t6lUEzqIfvP62TuV3nSL8mbIuqeC0k/KqTEMfudqHl9xqFXrwhGjtlHqgpX
BpGiV3fgeC+PAgMBAAGjggO+MIIDujCBjQYIKwYBBQUHAQEEgYAwfjBXBggrBgEFBQcwAoZLaHR0
cHM6Ly93d3cubG9nYWx0cS5lcy9jZXJ0aWZpY2F0ZWF1dGhvcml0eS9Mb2dhbHR5UXVhbGlmaWVk
Q0FHMS5jYWNlcnQuY3J0MCMGCCsGAQUFBzABhhdoHRwOi8vb2NzcEUubG9nYWx0eS5lczAdBgNV
HQ4EFgQUhrT4z3WcAYn4+lpzzg8RdIB7fswDAYDVR0TAQH/BAIwADADBgNVHSMEGDAWgBQmnST6l
r/dSTqUKFdb4Rs4o1LibDCCAQEGCCsGAQUFBwEDBIH0MIHxMBUGCCsGAQUFBwsCMAkGBwQAi+xJ
AQIwCAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYEAI5GAQYwCQYHBACORgEGAjCBqwYGBACORgEF
MIGgME4WSGh0dHBzOi8vd3d3LmxvZ2FsdHkuZXMvY2VydGlmaWNhdGVhdXRob3JpdHkvZW4vTEdU
X1BEU19yZWNlcHRvcvS2MXIwLnBkZhMCZW4wThZIaHR0cHM6Ly93d3cubG9nYWxoeS5lcy9jZXJ0
aWZpY2F0ZWF1dGhvcml0eS9lcy9MR1RfUERTX3JlY2VwdG9yLnYxcjAucGRmEwJlczCCAQUGA1Ud
IASB/TCB+jCB7AYLKwYBBAGB7AIBAwMwgdwwNQYIKwYBBQUHAgEWKWh0dHBzOi8vd3d3Lmxvz2Fs
dHkuZXMvUEuIL2RvY3VlZWS0YWNpb24vMIGiBggrBgEFBQcCAjCBlR6BkgBDAGUAcgB0AGkAZgBp
AGMAYQBkAG8AIABjAHUAYQBsAGkAZgBnAGMAYQBkAG8AIABkAGUAIABzAGUAbABsAG8AIABlAGwA
ZQBjAHQAcgDzAGdAaQBjAG8AIABhAHYAYQBuAHoAYQBkAG8AIABkAGUAIABwAGUAcgBzAG8AbgBh
ACAAagB1AHIA7QBkAGkAYwBhMAkGBwQAi+xAAQEwfQYDVR0fBHYwdDA4oDagNIYyaHR0cDovL2Ny
bDEubG9nYWx0eS5lcy9xdWFsaWZpZWRMb2dhbHR5U3ViQ0EwMi5jcmwwOKA2oDSGMmh0dHA6Ly9j
cmwyLmxvZ2FsdHkuZXMvcXVhbGlmaWVkTG9nYWx0eVN1YXNBMDIuY3JsMA4GA1UdDwEB/wQEAwIF
4DAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwHgYDVR0RBBcwFYETaWx5mbyJ5YUBsb2dh
bHR5LmNvbTANBgkqhkiG9w0BAQsFAAOCAgEAGQsInGs31ow2xZp1RyQGlakkm9veWWUzQnzpgUw1
mOFNSR9xlhCC/Ra9RoqLhQH4cHzFdwOQRYSAu8ErXSA/VL0mvrv4JLe9Yx0Qp2cN2Bt9yFOK4JPT
4rnMAkGwszgNwyR52OMVDHSyfhcs4y9dozrS5zXLjcoL9nWyQvK31K9tiCsCShEIbLpShqJj2QV
CRKbKMd4/ThZmCbnY/+z+iWS57dvbXiIC2yHoc9Ij4UQx/EfWV1NimQ1ICXyibsnH7cU88KzDWX
lPi6dSrQcR5qnBsxm2KvvEDKVNKUZvEDVd1BDOmplMwYYGzR7UF5FINZeBwiUe2zRS2d84mPx3Y
gxIesD3n1yFV+laCauqm0UegIyH8/PLrvyO94U6u2E2estqLxT95CNJRw6VyKgXjiVzJwnH+mtH
ErVP2puZ/A+Yj+upaR6OOXDzS1qrUNdg7L6LVI4KsEATDF/7KZ+g/MI2+SWT1iN/CpRjK21I+8U56
EtSTRw4bR1kIFygNMAAURUMXyC/mpXXNvAB3+I2I+rc0lUSSPg+pAU7A19hKLyH02lUSrd44
TVHPWVz4gR+Ab4CwfuaGTQ1Y20j1jDg4tyx4+2moXQx8UkmuFUltgaRPMuIGXwpC+piZqwEFF9ux
tb0e1vYjl6EpxlEiRZSjv3VhMqXa8bZZPeQ=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer C:	*ES*
Issuer ST:	*Madrid*
Issuer L:	*Alcobendas*
Issuer O:	*Logalty Servicios de Tercero de Confianza SL*
Issuer 2.5.4.97:	*VATES-B84492891*
Issuer OU:	*Logalty Trust Services*
Issuer CN:	*Logalty Qualified CA G2*
Subject C:	*ES*
Subject L:	*Alcobendas*
Subject O:	*Logalty Servicios de Tercero de Confianza SL*
Subject 2.5.4.97:	*VATES-B84492891*
Subject OU:	*Logalty Trust Services*
Subject SERIAL NUMBER:	*B84492891*
Subject CN:	*Sello de entrega electrónica certificada cualificada de Logalty*
Valid from:	*Wed Sep 12 11:08:48 CEST 2018*
Valid to:	*Sat Sep 11 11:08:48 CEST 2021*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:95:FF:37:7B:7E:2C:D9:70:D9:10:EA:BD:AA:D1:B2:E0:6F:0E:7F:D7:87:47:E0:F0:CC:35:D9:6D:9F:A4:E4:D5:9E:85:AD:45:AD:61:B4:F1:83:1E:06:B6:A9:E5:E6:36:AD:8F:9A:B7:2E:05:8A:56:0D:09:FA:12:65:76:39:40:89:6D:93:1F:84:76:2A:DB:C1:5F:4A:47:C2:BC:08:F9:87:33:AC:37:1A:3F:1C:41:EF:8A:87:EE:EC:64:71:B0:32:40:C8:C2:34:22:D0:22:35:F6:BF:CD:BD:9E:07:EB:5D:8C:C4:32:75:AD:FB:5F:5C:3A:CD:08:F1:A6:A3:53:CF:E5:D1:75:26:DA:98:01:D9:6F:A3:DA:A9:C5:50:08:95:8F:0C:27:80:1E:D1:AE:EB:99:8A:CD:0B:0E:7E:33:F3:37:72:9E:91:6A:85:97:33:98:75:D2:0D:C4:F7:D8:25:58:41:36:AE:DA:6D:19:B9:95:76:CB:70:D3:E6:CB:0C:9E:66:CA:11:E3:6D:B6:B0:AD:F2:25:04:CE:A2:1F:BC:FE:B6:4E:E5:77:9D:22:C1:99:B2:2D:A9:E8:02:7F:C9:3F:2A:A4:C4:32:5B:9D:A8:72:7D:72:A1:57:B7:08:46:82:D2:47:AA:AA:57:06:91:A2:57:77:E0:78:2F:8F:02:03:01:00:01*
Authority Info Access	*https://www.logalty.es/certificateauthority/LogaltyQualifiedCAG1.cacert.crt* *http://ocsp1.logalty.es*
Subject Key Identifier	*86:D4:F8:CF:75:9C:01:89:F8:FA:58:DE:8B:38:3C:05:D0:C1:EC:8B*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*

Certificate Policies	*Policy OID: 1.3.6.1.4.1.30210.1.3.3* *CPS pointer: https://www.logalty.es/PKI/documentacion/* *CPS text: [Certificado cualificado de sello electrónico avanzado de persona jurídica]* *Policy OID: 0.4.0.194112.1.1*
CRL Distribution Points	*http://crl1.logalty.es/qualifiedLogaltySubCA02.crl* *http://crl2.logalty.es/qualifiedLogaltySubCA02.crl*
Extended Key Usage	*id_kp_clientAuth*
Subject Alternative Name	*info.ca@logalty.com*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*92:B6:E3:71:3C:78:86:89:D6:52:E7:59:83:6C:D9:6E:75:85:BF:B5:A1:CC:DE:22:D7:F2:1E:80:A3:4E:88:01*

X509SubjectName

Subject C:	*ES*
Subject L:	*Alcobendas*
Subject O:	*Logalty Servicios de Tercero de Confianza SL*
Subject 2.5.4.97:	*VATES-B84492891*
Subject OU:	*Logalty Trust Services*
Subject SERIAL NUMBER:	*B84492891*
Subject CN:	*Sello de entrega electrónica certificada cualificada de Logalty*

X509SKI

X509 SK I	*htT4z3WcAYn4+ljeizg8BdDB7Is=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-04-05T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI	*[es]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

31.4 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU006

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU006*

Name *[en]* *Qualified timestamps issued by Logalty Qualified TSA TSU006*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5762382065790029706*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJ5zCCB8+gAwIBAgIIT/gX9Vt/D4owDQYJKoZIhvcNAQENBQAwgccxIDAeBgNVBAMMF0xvZ2Fs
dHkgUXVhbGlmaWVkIENBIEcyMR8wHQYDVQQLDBZMb2dhbHR5IFRvdXN0IFNlcnZpY2VzMRgwFgYD
VQRhDA9hQVRFUy1CODQ0OTI4OTExNTAzBgNVBAoMLExvZ2FsdHkgU2VydmlqW9zIGRlIFRlcmNl
cm8gZGUgQ29uZmlhbnphIFNMMRMwEQYDVQQHDApBbGNvYmVuZGFzMQ8wDQYDVQQIDAZNYWRyaWQx
CzAJBgNVBAYTAkVTMB4XDTIwMTIxMDEzNTYzMVoXDTI1MTIwOTEzNTYzMVowgcMxJTAjBgNVBAMM
HExvZ2FsdHkgUXVhbGlmaWVkIFRTQSBUU1UwMDYxHzAdBgNVBAsMFkxvZ2FsdHkgVHJ1c3QgU2Vy
dmlzZXMxGDAWBgNVBGEMD1ZBVEVTLUI4NDQ5MjgsMTEsMCoGA1UECgwjTG9nYWxtbSBQcnVlYmEg
cG9yIEludGVyc G9zaWNpb24gU0wxEzARBgNVBAcMCkFsY29yZWS kYXMxDzANBgNMBk1hZHJp
ZDELMAkGA1UEBhMCRVMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCTghBAPNaJ0bUM
l0yxcGRSvCyZKPHODsbq5MpGIsi6m7Sn+8MVNRt4DkW46X2aj0MoPmCQxOIrjAcZtQk4mujLOj8
dOGsqo5Zs9ozdSBms4N2+EkL1FJMjgOFPH8XP7iZy1snGMPobRn4ITmXgZ0Y yKktxva4+Drtm/6
hCR2CAFocw5g/3+b25RKkMd4E9kdb6EQgypBAWr2IG1MGcaGF+xIkjXRUNoQA3DSnBcE1bvgpbtG/
Pa2WTpZutd9lB+E3kojL23/1kml7S5BcD0A0WhRRsDq2oBAyh9blgsu6+Yy6D7uVYI/ooCTVv0q3
RcFwcWDcqaABD4VPijs/moEnR/Riy9hk/JjkzfuN0XbehyaBFpwNTnTJGmwLhdI1mJ0DxfTU/ZLV
6kAos2jI81KKewaLE2vDBNEVNN6evRxKDb4M2E88A5UkTGOqAz+gJS9BaPzhg/CqRBCjb55dEKj
ASl7ltg/4AtmC29mCmrIZso+RLZs7I01YXISKVs1T4COP0lUvzomzqLnQAmuYcJhig+j7d6XV8T
m8VjO3On09xPgr29pfp3bPkQpT47qsb1ZBYJ/OoXKEummIJFfPWDZPxfzuVTmFbtzNJIPUThgCcB
So6KRHZ/z/gPrppP6l7W/JU03DbC/c7kToVwVuuE1wnfnfujp31waPuu5Tf6FQIDAQABo4ID1zCC
A9MwHwYDVR0jBBgwFoAUlkk+pa/3ZUk6lChXW+EbOKNS4mwwgYQGCCsGAQUFBwEBBHgwdjBPBggr
BgEFBQcwAoZDaHR0cDovL2NvdC5sb2dhbHR5LmVzL2NlcnRpZmlyXRlYXVlaG9yaXR5LzcvZ2Fs
dHlRdWFsaWZpZWRDQUcyLmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AxLmxvZ2FsdHkuZXMw
ggF+BgNVHSAEggF1MIIBcTAJBgcEAIvsQAEBMIIBYgYLKwYBBAGB7AIBBQEwggFRMIIBEgYIKwYB
BQUHAgIwggEEHoIBAABDAGUAcgB0AGkAZgBpAGMAYQBkAG8AIABjAHUAYQBsAGkAZgBpAGMAYQBk
AG8AIABkAGUAIABzAGUAbABsAG8AIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8AIABkAGUAIABwAGUA
cgBzAG8AbgBhACAAagB1AHIA7QBkAGkAYwBhACAAcABhAHIAYQAgAGwAYQAgAGUAcABwAGUAZABp
AGMAaQDzAG4AIABkAGUAIABzAGUAbABsAG8AcwAgAGMAdQBhAGwAaQBmAGkAYwBhAGQAbwBzACAA
ZABIACAAdABpAGUAbQBwAG8AIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8wOQYIKwYBBQUHAgEWLWh0
dHBzOi8vd3d3LmxvZ2FsdHkuY29tL2NlcnRpZmlyXRlYXVlaG9yaXR5LzAWBgNVHSUBAf8EDDAK
BggrBgEFBQcDCDCB4AYIKwYBBQUHAQMEgdMwgdAwCAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYE
AI5GAQYwCQYHBACORgEGAjCBoQYGBACORgEFMIGWMEkWQ2h0dHBzOi8vd3d3LmxvZ2FsdHkuZXMv
Y2VydGlmaWNhdGVhdXRob3JpdHkvZW4vTEdUX1BEU19UU0EudjFyMC5wZGYTAmVuMEkWQ2h0dHBz
Oi8vd3d3LmxvZ2FsdHkuZXMvY2VydGlmaWNhdGVhdXRob3JpdHkvZXMvTEdUX1BEU19UU0EudjFy
MC5wZGYTAmVzMH0GA1UdIwR2MHQwOKA2oDSGMmh0dHA6Ly9zcmwxLmxvZ2FsdHkuZXMvcXVhbGlm
aWVkTG9nYWx0cVN1YkNBMDIuY3JsMDigNqA0hjodHRwOi8vY3JsMi5sb2dhbHR5LmVzL3F1YWxp
ZmlfZExvZ2FsdHlTdWJDQTAyLmNybDAdBgNVHQ4EFgQUhjiW3Ph3BJBxHxUtgQ/9sy1Hpn4wDgYD
VR0PAQH/BAQDAgeAMA0GCSqGSIb3DQEBDQUAA4ICAQAo/NqkuUdIDsTyo6M7x9BQmkc1C0TYoMBKg
6vYM4iWgKOqhwy7uVSwypur4dzcIpcjaHaowGiwG/r+R9XTRcjONASirytSv85UBbVSq+auXK
kqlcidEmDT04CSxMRzkVirUpbTqMWKVraw5r08Y83jH+X+5ovrwiJK6v4gKBzlH9oqiRdI6iz6o
lEtxQIOb1azQ47Q8S6GMJAg23mVxbgYkmu/RXPbrODbMLPmtheV8bdrWMbGj1xqz9+4tN8uIRtB
4yIdHV3WmqHP8ptY3mcon0WI2OK6DFqjg4b6fp4ePI8RT05TKF1G5NOC5TDdmaTMyTtvUeaqASp
qHC3Rzzrslg8Rc3boBeIQgtI3z66ULQxmJFoZp6dZQpjpGFIjI7/THp07I8tUBRGybsuYxAZ9kmy
k3AIVmj+N4Sok7ekNNmcQllqahXy43FsqJzQ/PgykLR374lsXnX5AKqqO3bK2F4+C7RfeSF+MMd
k1DEuCAMbXKEikk/jHuihV/oP3HMZSPdR/FGWSp3dzmrjdA+Lx4S+r+eTCqEVvXzdn1sS/odxUPP
OmJM+OOTAo0RcVSGsmsRkWcsWGKUjncyOyZaQfsdimugS9bXNt2+CwD1LMtz4tkqjOnd4LKsWsbp
7k9ZNaexHtayCp6SRwNt5ZNfXeCcDJO5P56TWN3Vw==

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *Madrid*

Issuer L: *Alcobendas*

Issuer O: *Logalty Servicios de Tercero de Confianza SL*

Issuer 2.5.4.97: *VATES-B84492891*

Issuer OU:	*Logalty Trust Services*
Issuer CN:	*Logalty Qualified CA G2*
Subject C:	*ES*
Subject ST:	*Madrid*
Subject L:	*Alcobendas*
Subject O:	*Logalty Prueba por Interposicion SL*
Subject 2.5.4.97:	*VATES-B84492891*
Subject OU:	*Logalty Trust Services*
Subject CN:	*Logalty Qualified TSA TSU006*
Valid from:	*Thu Dec 10 14:56:31 CET 2020*
Valid to:	*Tue Dec 09 14:56:31 CET 2025*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:93:82:10:40:3C:D6:89:D1:B5:0C:23:4C:B1:78:64:52:BC:2C:99:28:F1:CE:0E:C6:EA:E4:CA:46:22:C8:BA:9B:B4:A7:FB:C3:15:35:1B:78:0E:45:B8:E9:7D:9A:8F:43:28:3E:60:90:C4:E2:2B:FE:30:1C:66:D4:24:E2:6B:A3:2C:E8:FC:74:E1:AC:AA:8E:59:B3:DA:33:75:20:66:B3:83:76:F8:49:0B:D4:52:4C:8E:03:85:3C:7B:7C:5C:FE:E2:67:2D:6C:9C:63:0F:A1:B4:67:E0:84:E6:5E:06:74:62:22:A4:B7:1B:DA:E3:E0:EB:D2:6F:FA:84:24:76:08:01:68:73:0E:60:FF:7F:9B:DB:94:4A:F2:43:38:13:D9:1D:E8:44:20:BE:90:40:5A:BD:AD:1B:53:06:71:A1:85:FB:12:24:8D:74:54:36:84:00:DC:34:A7:05:C1:35:86:F8:29:6E:D1:BF:3D:AD:96:4E:96:6E:B5:DF:65:07:E1:37:92:88:CB:DB:7F:F5:92:69:7B:4B:90:5E:0F:40:34:5A:14:51:B0:3A:B6:A0:10:32:87:D6:E5:82:CB:BA:F9:8C:BA:0F:BB:95:62:5F:E8:A0:24:D5:BF:4A:B7:45:C1:70:71:60:DC:A9:A0:01:0F:85:4F:8A:3B:3F:9A:81:27:47:F4:62:CB:D8:64:FC:98:E4:CD:FB:8D:D1:76:DE:87:26:81:16:9C:0D:4E:74:C9:1A:6C:0B:85:D9:75:98:9D:03:C5:F4:D4:FD:92:D5:EA:40:28:B3:68:DF:F3:52:8A:7B:06:8B:13:6B:C3:04:D1:15:34:DE:9E:BD:1C:4A:0D:BE:0C:D8:4F:3C:03:95:24:4C:63:AA:03:3F:A0:25:2F:41:68:FC:E1:83:F0:BF:A9:10:42:8D:BE:79:74:42:A3:01:29:7B:7E:D8:3F:E0:07:E6:09:9F:66:0A:6A:C9:DA:CA:3E:44:B6:73:EC:8D:35:B5:85:E5:48:A5:6C:D5:3E:02:38:FD:25:52:FC:E8:9B:3A:8B:9D:00:27:B9:87:09:86:28:3E:8F:B7:7A:5D:5F:13:9B:C5:63:3B:73:A7:D3:DC:4F:AA:BD:BD:A5:FA:77:6C:F9:10:A5:3E:3B:AA:C6:F5:64:16:09:FC:EA:17:28:4B:A6:98:82:45:7C:F5:83:64:FC:5F:CE:E5:53:98:56:ED:CC:D2:48:3D:44:E1:80:27:01:4A:8E:8A:44:76:7F:CF:F8:0F:AE:9A:4F:EA:5E:D6:FC:95:34:DC:38:42:FD:EE:E4:4E:85:70:56:EB:84:D7:09:DF:9D:FB:A3:A7:7D:70:68:FB:AE:E5:37:FA:15:02:03:01:00:01*
Authority Key Identifier	*26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*
Authority Info Access	*http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt* *http://ocsp1.logalty.es*
Certificate Policies	*Policy OID: 0.4.0.194112.1.1* *Policy OID: 1.3.6.1.4.1.30210.1.5.1* *CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]* *CPS pointer: https://www.logalty.com/certificateauthority/*
Extended Key Usage	*id_kp_timeStamping*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
CRL Distribution Points	*http://crl1.logalty.es/qualifiedLogaltySubCA02.crl* *http://crl2.logalty.es/qualifiedLogaltySubCA02.crl*
Subject Key Identifier	*86:38:96:DC:F8:77:04:90:71:1F:15:2D:81:0F:FD:B3:2D:47:A6:7E*
Key Usage:	*digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D0:0B:B9:7B:7A:BA:BF:95:F5:78:A8:63:95:BA:8B:01:6B:C1:79:8C:57:40:08:12:D7:31:17:97:A0:A2:C1:C2*

X509SubjectName

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU006*

X509SKI

X509 SK I *hjiW3Ph3BJBxHxUtgQ/9sy1Hpn4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-03-17T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

31.5 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU007

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU007*

Name *[en]* *Qualified timestamps issued by Logalty Qualified TSA TSU007*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *8216736880441155060*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJ8TCCB9mgAwIBAgIcge2qJuL3fQwDQYJKoZIhvcNAQENBQAwgccxIDAeBgNVBAMMF0xvZ2Fs
dHkgUXVhbGlmaWVkIENBIEcyMR8wHQYDVQQLDBZMb2dhbHR5IFRydXN0IFNlcnZpY2VzMRgwFgYD
VQRhDA9WQVRFUy1CODQ0OTI4OTExNTAzBgNVBAoMLExvZ2FsdHkgU2VydmljaW9zIGRlIFRlcmNl
cm8gZGUgQ29uZmlhbnphIFNMMRMwEQYDVQQHDApBbGNvYmVuZGFzMQ8wDQYDVQQIDAZNYWRyaWQx
CzAJBgNVBAYTAkVTMB4XDTIxMDQwNzEzMjIwMloXDTI2MDQwNjEzMjIwMlowgcMxJTAjBgNVBAMM
HExvZ2FsdHkgUXVhbGlmaWVkIFRTQSBUU1I1wMDcxHzAdBgNVBAsMFkxvZ2FsdHkgVHI1c3QgI2Vy
dmljZXMxGDAWBgNVBGEMD1ZBVEVTLUI4NDQ5Mjg5MTEsMCoGA1UECgwjTG9nYWx0eSBQcnVlYmEg
cG9yIEludGVycG9zaWNpb24gU0wxEzARBgNVBAcMCkFsY29iZWSkYXMxDzANBgNVBAgMBk1hZHJp
ZDELMAkGA1UEBhMCRVMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDGx29q228MDbvf
vDxFi36WAORmCsc36ij/DN4JCYcFm5kbMG+lkBuDZHSAdSea7Evlqs9lVBS+QMZfpNFzgHpP+Vq
0hbEhgLbDvw7OjO0SIo9LNyfLSsyaYthj2YYqU+HRjR6DbMI8zusRSCpZWRLe+GnK3rxpjDEoZSH
LbaLfQ8PACUacLiAZuFAKwyV/FAN3k2b6atFCkMIGLaDT348XtfdYbCbiU8bBFdd0NaBbm4hmFdh
tV4df9aUC+ve9QDxYKdsqCJ4BXJV2r2DRKMRAwKpsml7qSYDDq8wMTKKzqpGkQ9kbKqK3kT5STCx
6xRjRjESwvayMFCr16tTh65JWe2JeHBefnPL6NCtqJwWH0kDD4zeo9RzWjzYdDi7sbcG74uKGY
b2NQSmRxIlP7x24XZ2dVH0j0/8+ttSLekHvKlbNQ0CK/I3rbGXsVdURxKaqkgNGCzNSgfX0anBV
bIOEziKsLx8wuQkiCrE6wm8aXIiF3qK6l/9c+OpsiMOSzJ9WhJxv6dggQqEVWnPCg53CPa2emr8K
ET5VvnjtI2xo9ERbKRZpMPAAMZQ5WSsO8WiimSld9MkzwjcsNy94aaPY83qlNh9wUB5x7Ujo7yRa
zqTYLP5YnVU76BEzqJSaJIS+4I+oKv16xwhNFxrI7vSm3OiuEHkTHoZQFRPq9wIDAQABo4ID4TCC
A90wHwYDVR0jBBgwFoAUIkk+pa/3ZUk6lCbXW+EbOKNS4mwwgYQGCCsGAQUFBwEBBHgwdjBPBggr
BgEFBQcwAoZDaHR0cDovL2NydC5sb2dhbHR5LmVzL2NlcnRpZmljYXR1YXV0aG9yaXR5L0xvZ2Fs
dHlRdWFsaWZpZWRDQUcyLmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AxLmxvZ2FsdHkuZXMw
ggF+BgNVHSAEggF1MIIBcTAJBgcEAIvsQAEBMIIBYgYLKwYBBAGB7AIBBQEwggFRMIIBEgYIKwYB
BQUHAgIwggEEHoIBAABDAGUAcgB0AGkAZgBpAGMAYQBkAG8AIABjAHUAYQBkAGkAZgBpAGMAYQBk
AG8AIABkAGUAIABzAGUAbABsAG8AIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8AIABkAGUAIABwAGUA
cgBzAG8AbgBhACAAagB1AHIA7QBkAGkAYwBhACAAcABhAHIAYQAgAGwAYQAgAGUAcABwAGUAZABp
AGMAaQDzAG4AIABkAGUAIABzAGUAbABsAG8AcwAgAGMAdQBhAGwAaQBmAGkAYwBhAGQAbwBzACAA
ZABlACAAdABpAGUAbQBwAG8AIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8wOQYIKwYBBQUHAgEWLWb0
dHBzOi8vd3d3LmxvZ2FsdHkuY29tL2NlcnRpZmljYXR1YXV0aG9yaXR5LzAWBgNVHSUBAf8EDDAK
BggrBgEFBQcDCDCB6gYIKwYBBQUHAQMEgd0wgdowCAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYE
AI5GAQYwCQYHBACORgEGAjCBqwYGBACORgEFMIGgME4WSGb0dHBzOi8vd3d3LmxvZ2FsdHkuY29t
L2NlcnRpZmljYXR1YXV0aG9yaXR5L3Bkcy9lb9MR1RtUERTX1RTQY92MXI0LnBkZbMCZW4wTbZI
aHR0cHM6Ly93d3cubG9nYWx0eS5jb20vY2VydGlmaWNhdGVhdXRob3JpdHkvcGRzL2VzL0xlHVF9Q
RFNfVFNBX3YxcjQucGRmEwJlczB9BgNVHR8EdjB0MDigNqA0hjJodHRwOi8vY3JsMS5sb2dhbHR5
LmVzL3F1YWxpZmllZExvZ2FsdHlTdW/JDQTAyLmNybDA4oDagNiYvaHR0cDovL2NybDIubG9nYWx0
cS5lcy9sdWFsaWZpZWRMb2dhbHR5U1VzQ0EwMzSjcmwwHQYDVR0OBBYEFIVO+T36EBCguQKWZC0
JLqxN+KSMA4GA1UdDwEB/wQEAwIHgDANBgkqhkiG9w0BAQ0FAAOCAgEAvS1Hf+45pK4tk8rY9vI1
9eHVJPsUm7Xb4SMYGQY11GlmhXy3LYQ/pxIxInPubF3Q4ljyAVRH8o5KD06Pon6/clqy4sxxieDJY
7Tqb+bZ1/smpvb0OAHhniaSJE4lc68XG+3hUKjt52dIkjOwrVrYIoB/RL0Vd1Msyqa9FUIte5qB
3BKmv2CyGcwCSEz9/rj28m2aXFzt3bd8k1yOwlhEJskG+dYFEh6mqL1xLLgCXDWQHmxDmmtvq3cf
v8N1EcJrhdNzIiKvy9XIcyXOER6tgvCgrTyJQV7vaGiryKHpdD9HmJSFLAJaw1eqzS+iSDrsIj3a
M/qvKe+UTqDVFTKD8zDSIS3bdcd4drAem24OVyrZs/M4FNyRtg2WM51twQkZOZ0+wy+clPBp7mE
cd9PEoAfRM0L6Zn V6DK+RGRLcjjIGZLIKmYySF0JP9w51psFd9XoBQJAOo/3mkhIwNXz3kcVtBK
MUh/b2O7SqW1JSDGHZioT0Uc5vsxxuQGCzxKZeCHYvNt9sRQyQFHN5grPXkc2hiTChV3I3GwA5a+
tM99I6N0XY2Bak7NKaoKTkToSY+ZS7p6O2qBr0ttDXtoo/F4TQbQq9QADK/wsg+kHLzbSucAKP
I6O9ZV4YEnVytKs3vzoXN+jnvsIMnVNytHXxahjkWs0q2oc13tkPOoo=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *Madrid*

Issuer L: *Alcobendas*

Issuer O: *Logalty Servicios de Tercero de Confianza SL*

Issuer 2.5.4.97: *VATES-B84492891*

Issuer OU: *Logalty Trust Services*

Issuer CN: *Logalty Qualified CA G2*

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU007*

Valid from: *Wed Apr 07 15:22:02 CEST 2021*

Valid to: *Mon Apr 06 15:22:02 CEST 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C6:C7:6F:6A:DB:6F:0C:0D:BB:DF:C8:3C:45:8B:7E:96:00:E4:66:0A:C7:B7:EA:38:FF:0C:DE:09:09:87:85:9B:99:1B:30:6F:9F:90:1B:83:66:21:D2:01:D4:9E:6B:B1:32:22:3A:BD:95:50:52:F8:E3:19:22:93:45:CE:01:E9:3F:E5:6A:D2:16:C4:86:02:DB:0E:FC:3B:3A:33:B4:48:8A:3D:2C:DC:9F:2D:2B:32:69:8A:E1:8F:66:18:A9:4F:87:46:34:7A:0D:B3:1F:F3:3B:AC:45:20:A9:65:64:4B:7B:E1:A7:93:7A:F1:A6:30:C4:A1:94:87:2D:B6:8B:7D:0F:0F:00:25:1A:70:B8:80:66:E1:40:2B:0C:95:FC:50:0D:DE:4D:9B:E9:AB:45:0A:43:08:18:B6:83:4F:7E:3C:5E:D7:DD:61:B0:9B:89:4F:1B:04:57:5D:D0:D6:81:6E:6E:21:98:57:61:B5:5E:1D:7F:D6:94:0B:EB:DE:F5:00:F1:60:A7:6C:A8:22:78:05:72:55:DB:3D:83:44:A3:11:03:02:A9:B2:62:3B:A9:26:03:0E:AF:30:31:32:8A:CE:AA:46:91:0F:64:84:A:8A:DE:44:F9:49:30:B1:EB:14:63:46:31:12:C2:F8:9A:C8:C1:42:AF:5E:AD:4E:11:B9:25:6E:B6:25:E1:FC:79:F9:CF:2F:A3:42:B6:A9:63:C1:61:F4:90:30:F8:CD:EA:3D:47:35:A3:CD:8E:83:8B:BB:1B:70:6E:F8:C6:41:98:6:F:63:50:4A:64:71:22:53:FB:C7:6E:17:67:67:55:1F:48:F4:FF:FF:3E:7E:D4:8B:7A:41:EF:2A:56:CD:43:40:8A:FC:8D:EB:6C:65:EC:55:D5:11:C4:A6:AA:92:03:46:0B:33:52:81:F5:F4:6A:70:55:6C:83:84:CE:22:AC:2F:1F:30:B:9:09:22:0A:B1:3A:C2:6F:1A:5C:88:85:DE:A2:BA:97:FF:5C:F8:EA:6C:88:C3:92:CC:9F:56:84:9C:6F:E9:D8:20:42:A1:15:5A:73:C2:83:9D:C2:3D:AD:9E:9A:BF:0A:11:3E:55:BE:78:ED:97:6C:68:F4:44:61:29:16:69:30:F0:00:31:94:39:59:2B:0E:F1:68:9F:9A:C9:5D:F4:C9:33:C2:37:22:37:2F:78:69:A3:D8:F3:7A:88:36:1F:70:50:1E:71:ED:48:E8:EF:24:5A:CE:A4:D8:2C:FE:58:9D:55:3B:E8:11:33:A8:9F:1A:27:54:BE:E2:5F:A8:2A:FD:7A:C7:08:4:D:17:1A:E5:EE:F4:A6:DC:EF:EE:10:79:13:1E:86:50:15:13:DA:F7:02:03:01:00:01

Authority Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

Authority Info Access

http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt

http://ocsp1.logalty.es

Certificate Policies

Policy OID: 0.4.0.194112.1.1

Policy OID: 1.3.6.1.4.1.30210.1.5.1

CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]

CPS pointer: https://www.logalty.com/certificateauthority/

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points

http://crl1.logalty.es/qualifiedLogaltySubCA02.crl

http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

Subject Key Identifier *85:4E:F9:3D:FA:10:11:A0:B9:02:96:B5:90:B4:24:BA:B1:37:E2:92*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *41:06:46:45:E1:06:1E:A5:87:8B:12:43:EA:82:B2:C1:1C:11:71:B7:F4:CC:F3:01:E3:6C:88:B5:8D:DF:A8:A6*

X509SubjectName

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU007*

X509SKI

X509 SK I *hU75PfoQEaC5Apa1kLQkurE34pI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-07-01T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

31.6 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU008

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU008*

Name *[en]* *Qualified timestamps issued by Logalty Qualified TSA TSU008*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6138734566089258641*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJ8TCCB9mgAwIBAgIIVTEqkD4pdpEwDQYJKoZIhvcNAQENBQAwgccxIDAeBgNVBAMMF0xvZ2Fs
dHkgLXVhbGlmaWVkIENBIEcyMR8wHQYDVQQLDBZMb2dhbHR5IFRvdXN0IFNlenZpY2VzMRgwFgYD
VQRhDA9WQVRFUy1ICODQOOT4OTExNTAzBgNVBAoMLExvZ2FsdHkgI2VydmlzW9zIGRlIFRlcmNl
cm8gZGUgQ29uZmlhbnphIFNMMRMwEQYDVQQHDApBbGNvYmVuZGFzMQ8wDQYDVQQIDAZNYWRyaWQx
CzAJBgNVBAYTAkVTMB4XDTIxMDQwNzEzMjgzN1oXDTI2MDQwNjEzMjgzN1owgcMxJTAjBgNVBAMM
HExvZ2FsdHkgUXVhbGlmaWVkIFRTQSBUU1UwMDgxHzAdBgNVBAsMFkxvZ2FsdHkgVHJ1c3QgU2Vy
dmlqZXMxGDAWBgNVBGEMD1ZBVEVTLU4NDQ5Mjg5MTEsMCwGA1UECgwJTG9nYWxtcSBQcnVlYmEg
cG9yIEludGVycG9zaWNpb24gU0wxEzARBgNVBAcMCkFsY29lZW5kYXMxDzANBgNVBAgMBk1hZHJp
ZDELMAkGA1UEBhMCRVMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDqXRpjZ4myDFXJ
ArGrc11SiQIEbn9RsWxMZ/9ekPS0V/YyQky/n/BFJigZB0sVea7Ig7cxWnzuHVKWYp7bVeJV8n0e
WCSs8cDyCPE6ngHx5MYCcGi8d4AzQQr+Wzz8mYQFAEkQOUQAHPhoukaSoHDreg/orbW5BRJqnEpr
s37kuzHCdXbQuqvGLyVB96ai30w1aLuCNDa78SeD8ep5XCIEfQ0xlI0j+F6ubd3aNmy3DY/+wUWo
16MGlw3SGITSjcRLTgxhbmH1zzU9Iq6QS5GzLy01WgIVB6Vkmf7fyBrhPi6goPPVH0OBhFkw8xBu
1+8tJLcDWI3M29HjWmN/i4ugbyUdp5d0MOXnqAn8B22zAfDXcU2TXktp6WuvsX9d/FiTyyQ6jc9c
MEtvLI8VMoXXxS1I0IX0PQ7+VaVVKc14mq2FLoJt5AmnUCHWGufvOsyxbYr5yRtzzJmT+F89RHt
Y9t/8Fwd5V2CcLxc4P/pwh0zxBb+vmII8il8csePnzmtrHyOfD1RmeO/imtGirsL93p8TCAuggfs
5wXmGlRRG4nBakIfct5x3NEU0pJX3Wtv+/OKvunc1Rfzpgj9F3e44IU3zFonQPiwJztnnepqbMu
48I8FXdbCYBnOFXQEaq+2HlZuNd1ZniZG0i6vBPGpZqCTrUBX1L2i3VoACW/RQIDAQABo4ID4TCC
A90wHwYDVR0jBBgwFoAUJkk+pa/3ZUk6lCbXW+Eb0KN84mwwgYQGCCsGAQUFBwEBBHgwdjBPBggr
BgEFBQcwAoZDaHR0cDovL2NydC5sb2dhbHR5LmVzL2NlcnRpZmljYXRlYXV0aG9yaXR5L0xvZ2Fs
dHlRdWFsaWZpZWRDQUcyLmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AxLmxvZ2FsdHkuZXMw
ggF+BgNVHSAEggF1MIIBcTAJBgcEAIvsQAEBMIIBYgYLKwYBBAGB7AIBBQEwggFRMIIBEgYIKwYB
BQUHAgIwggEEHoIBAABDAGUAcgB0AGkAZgBpAGMAYQBkAGMAIAB2AHUAYQBsAGkAZgBpAGMAYQBk
AG8AIABkAGUAIABzAGUAbABsAG8AIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8AIABkAGUAIABwAGUA
cgBzAG8AbgBhACAAagB1AHIA7QBkAGkAYwBhACAAcABhAHIAYQAgAGwAYQAgAGUAcABwAGUAZABp
AGMAaQDzAG4AIABkAGUAIABzAGUAbABsAG8AcwAgAGMAdQBhAGwAaQBmAGkAYwBhAGQAbwBzACAA
ZABlACAAdABpAGUAbQBwAG8AIABlAGwAZQBjAHQAcgDzAG4AaQBjAG8wOQYIKwYBBQUHAgEWLWh0
dHBzOi8vd3d3LmxvZ2FsdHkuY29tL2NlcnRpZmlyYXRlYXV0aG9yaXR5LzAWBgNVHSUBAf8EDDAK
BggrBgEFBQcDCDCB6gYIKwYBBQUHAQMEgd0wgdowCAYGBACORgEBMAsGBgQAjkYBAwIBDzATBgYE
AI5GAQYwCQYHBACORgEGAjCBqwYGBACORgEFMIGgME4WSGhlQHBzOi8vd3d3LmxvZ2FsdHkuY29t
L2NlcnRpZmlyYXRlYXV0aG9yaXR5L3Bkcy9lbi9MR1RfUERTX1RTQV92MXI0LnBkZhMCZW4wThZI
aHR0cHM6Ly93d3cubG9nYWx0eS5hb0vY2VydGlmaWNhdGVhdXRob3JpdHkvcGRzL2VzLl0xIVF9Q
RFNlVFNBX3YxcjQucGRmEwJlczB9BgNVHR5EdjB0MDigNqA0hjJodHRwOi8vY3JsMS5sb2dhbHR5
LmVzL3F1YWxpZmllZExvZ2FsdHlTdWJDQTAyLmNybDA4oDagNlYyaHR0cDovL2NybDIubG9nYWx0
eSSlcy9xdWFsaWZpZWRMb2dhbHR5U3VtQ0EwMi5jcmwwHQYDVR0OBBYEFOHNPnFKM3w4QBQ6w7QN
1rbL0ScgMA4GA1UdDwEB/wQEAwIFgDANBgkqhkiG9w0BAQOFAAOCAgEAWFoydZ/g0SgGAQB6UpbO
AbcKzkKvNDMDQrjq2Bodv/kSCYIG+PF19VBYT89X1bEGmadSprKsRitfQFwTric3ZWUauvTxdS3Fr
9tp15Xn6U/nseqmQWWq2LyKhzAOlsZXZsJiSrpZXfsq/Yl3q/z1oRmHasmoTRKSFCNYyJEFEdGJnP
QZu1M6Jg8ZOu02hHgb/8aLFkPG04MTx3pArdk6UcBm6lVMvj5P/DgIpz3QMQ/3QX66LglnoEhwmS
b82T57x58jub+nFeu0J9+/cxHSSoEcB4MfjtBpofvQIEwNsvPMfMpkoIJESQSxPLSQRGjvc1O+d
J44uBMND9mPg2COvG7GWPXoLqi+5+ofDjmVcL+zqOWrMbpUoo0Mo0BH6kId5Nplu21JVV1VaiOon7
TefpxD6l6H/Izq0Ca6Xw7XUu9T2Ln22AJ4TUFoNdSNNNcDmvhHYkVJjwoZ/fi01hm85UcSyMZZ0
4HXDxzNy24syZCkVdp4dkuOvQf8CeSdisElrog2HCnlhlcVZzDu/tkupzZCSn0zxuHwQy4fC+wCF
JIv9IedE1Tfu+7c50R0T7yV+zWYJd2Ob/oAFXaW0yMWpFySLp133wt3vXtgD3trP7o/+tQSpHKh
1+7zlmNut62+x70xmhoAmVkQse4BYNnk2YEFpPnq20B/hjODMbFgZ4k=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *Madrid*

Issuer L: *Alcobendas*

Issuer O: *Logalty Servicios de Tercero de Confianza SL*

Issuer 2.5.4.97: *VATES-B84492891*

Issuer OU: *Logalty Trust Services*

Issuer CN: *Logalty Qualified CA G2*

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU008*

Valid from: *Wed Apr 07 15:28:37 CEST 2021*

Valid to: *Mon Apr 06 15:28:37 CEST 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EA:5D:1A:63:67:89:B2:0C:55:C9:02:B1:AB:73:5D:52:89:09:44:6E:7F:51:B1:6C:4C:67:FF:5E:90:F4:B4:57:F6:22:42:4C:BF:9F:F0:45:26:28:19:07:4B:15:79:A4:ED:81:37:31:5A:7C:EE:1D:52:96:62:9E:DB:55:E2:55:F2:7D:1E:58:2E:6C:F1:C0:F2:08:F1:3A:9E:A1:F1:E4:C6:02:78:67:FA:77:80:33:41:0A:FE:5A:BC:FC:99:84:05:00:49:10:39:44:00:1C:F8:68:BA:46:BC:A0:70:EB:7A:0F:E8:AD:B5:B9:05:12:6A:9C:4A:6B:B3:7E:E4:BB:31:C2:75:76:D0:BA:AB:C6:2F:25:41:F7:A6:A2:DF:4C:35:68:BB:82:34:36:BB:F1:27:83:F1:EA:79:5C:22:04:7D:0D:31:96:5D:23:F8:5E:AE:6D:DD:DA:36:6C:B7:0D:8F:FE:C1:45:A8:D7:A3:06:97:0D:D2:18:84:D2:8D:C4:4B:4E:0C:61:6E:61:F5:CF:35:3D:26:AE:90:4B:91:B3:2F:2D:35:5A:02:15:07:A5:64:99:FE:DF:C8:1A:E1:3E:2E:A0:A0:F3:D5:1F:43:81:84:59:30:F3:10:6E:D7:EF:2D:24:B7:03:58:8D:CC:DB:D1:E3:5A:63:7F:8B:8B:AA:6F:25:1D:A7:97:74:30:E5:E7:A8:09:FC:07:6D:B3:01:F0:D7:79:4D:93:5E:4B:69:E9:6B:AF:B1:7F:5D:FC:57:D3:CB:24:3A:8D:CF:5C:30:4B:6F:2E:5F:15:32:85:D7:B1:2D:44:D0:3D:0F:43:BF:95:69:55:4A:FD:ED:78:9A:AD:85:2E:82:6D:E4:09:A7:50:21:D6:1A:E2:2F:3A:CC:B1:85:8A:D2:C9:1B:73:88:9A:E7:4F:E1:7C:F5:11:ED:63:DB:7F:F0:5C:1D:E5:5D:82:70:BC:5C:E0:FF:E9:C2:1D:33:C4:16:FE:BE:62:08:F2:22:3C:72:C7:8F:9F:39:AD:AC:7C:8E:94:3D:51:99:E3:BF:8A:6B:46:8A:BB:0B:F7:7A:7C:4C:20:2E:82:07:EC:E7:05:E6:1A:54:51:1B:89:C1:6A:47:C8:7D:CB:79:C7:73:44:53:4A:49:5F:75:AD:BF:EF:CE:2A:FB:A7:73:54:5F:CE:9A:A3:F4:5D:DE:E3:82:14:DF:31:68:9D:03:E2:C0:9C:ED:9E:77:A9:A9:B3:2E:E3:C2:3C:15:77:5B:09:80:67:38:55:D0:11:AA:BE:D8:79:59:B8:D7:75:66:78:99:1B:48:BA:BC:13:C6:A5:9A:82:22:B5:01:5F:52:F6:8B:75:68:00:25:BF:45:02:03:01:00:01

Authority Key Identifier

26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C

Authority Info Access

http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt

http://ocsp1.logalty.es

Certificate Policies

Policy OID: 0.4.0.194112.1.1

Policy OID: 1.3.6.1.4.1.30210.1.5.1

CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]

CPS pointer: https://www.logalty.com/certificateauthority/

Extended Key Usage

id_kp_timeStamping

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points

http://crl1.logalty.es/qualifiedLogaltySubCA02.crl

http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

Subject Key Identifier

E1:CD:3E:71:4A:33:7C:38:40:14:3A:C3:B4:0D:D6:B6:D4:D3:97:20

Key Usage:

digitalSignature

Thumbprint algorithm:

SHA-256

Thumbprint:

89:DD:A8:76:2B:40:6C:5F:63:97:26:B8:43:7B:23:5B:1F:B9:67:2E:DC:70:C6:EA:65:90:8D:83:12:B8:15:34

X509SubjectName

Subject C:

ES

Subject ST:

Madrid

Subject L:

Alcobendas

Subject O:

Logalty Prueba por Interposicion SL

Subject 2.5.4.97:

VATES-B84492891

Subject OU:

Logalty Trust Services

Subject CN:

Logalty Qualified TSA TSU008

X509SKI

X509 SK I *4c0+cUozfDhAFDrDtA3WttTTlyA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-07-01T01:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

32 - TSP: LLEIDANETWORKS SERVEIS TELEMATICS, S.A.

.

TSP Name

Name	*[en]*	*LLEIDANETWORKS SERVEIS TELEMATICS, S.A.*
Name	*[es]*	*LLEIDANETWORKS SERVEIS TELEMATICS, S.A.*

TSP Trade Name

Name	*[en]*	*LLEIDA.NET*
Name	*[es]*	*LLEIDA.NET*
Name	*[en]*	*VATES-A25345331*
Name	*[es]*	*VATES-A25345331*
Name	*[en]*	*Lleidanetworks Serveis Telemàtics, S.A*
Name	*[es]*	*Lleidanetworks Serveis Telemàtics, S.A*

PostalAddress

Street Address	*[en]*	*C/ General Lacy, 42*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28045*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*C/ General Lacy, 42*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28045*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:info@lleida.net*

URI	*[en]*	*http://www.lleida.net/en*
URI	*[es]*	*mailto:info@lleida.net*
URI	*[es]*	*http://www.lleida.net/es*

TSP Information URI

URI	*[en]*	*http://www.lleida.net/en*
URI	*[es]*	*http://www.lleida.net/es*

32.1 - Service (granted): Servicio cualificado de entrega electrónica certificada "Openum eIDAS"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description	*[en]*	*An electronic delivery service providing qualified electronic deliveries.*
	[es]	*Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name	*[es]*	*Servicio cualificado de entrega electrónica certificada "Openum eIDAS"*
Name	*[en]*	*Qualified electronic registered delivery service "Openum eIDAS"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5379122206984586969*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGvjCCBaagAwIBAgIISqZ7Jb67RtkwDQYJKoZIhvcNAQELBQAwgZIxCzAJBgNVBAYTAkVTMR4w
HAYDVQQKExVGaXJtYXByb2Zlc2lvbmFsIFMuQS4xIjAgBgNVBAsTGUNlcnRpZmlj YWRvcyBDdWFs
aWZpY2Fkb3MxEjAQBgNVBAUTCUE2MjYzNDA2ODEnMCUGA1UEAxMiQUMgRmlybWFwcm9mZXNpb25b
bCAtIENVQUsJRkIDQURPUzzRaYMmd1SZM9gq5w7cRmDQQbSc/RDtnpkbiBcDcU/pxlbrgrQ6E
VQQGEwJFUzEPMA0GA1UECAwGTEvFSURBMTEwLwYDVQQKDChMbGVpZGFuZXR3b3JrcyBTZXJ2ZWlz
IFRlbGVtw6B0aWNzLCBTLkEuMRgwFgYDVQRhDA9WQVRFUy1BMjUzNDUzMzExHTAbBgNVBAsMFFRF
Q0hOSU NBTCBERVBHUlRNRU5UMRIwEAYDVQQFEwlBMjUzNDUzMzExMTAvBgNVBAMMKExsZWlkYW5l
dHdvcmtzIFNlcnZlaXMgVGVsZW3DoHRpY3MsIFMuQS4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDZHCJmq3VQiypncEMq9AJfvGlhY2/7siKr2kYToqrRMBWszQ8KnFjY8NRyFdS1xcjn
Y+dh55l4Ycy0pPgZy2fiodigN+bbGgbIOP0dPT92olTbyfiGyEkYyWQLwya7lqmagoZ0gGHYShSAZ
r2ssNu2bDxsHKp4dpedjMTFbp4eqQD89nSk7Mcd5WK0Cm0Zi7DTR3P/TuXS+blo8FAIOrUW3tCIp
LRYgj97YdcIDWduluvcXAt0/CRaYMmd1SZM9gq5w7cRmDQQbSc/RDtnpkbiBcDcU/pxlbrgrQ6E
uaIyuCQSk2kc/4h4+DeMW3bWb1Az1/KvzpoHn2NlxHArr s9AgMBAAGjggLVMIIC0TB6BggrBgEF
BQcBAQRuMGwwPAYIKwYBBQUHMAKGMGh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25bbC5jb20vY3Vh
bGlmaWNhZG9zLmNydDAsBggrBgEFBQcwAYYgaHR0cDovL29jc3AuZmlybWFwcm9mZXNpb25bbC5j
b20vHQYDVR0OBBYEFINzCJjrGBdmqucHp3zcmkHEsq1GMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
FoAUjHHMkwdv0dWGaH2COkHZTAL4ll0wfQYIKwYBBQUHAQMEcTBvMAgGBgQAjkYBATALBgYEAI5G
AQMCAQ8wEwYGBACORgEGMAkGBwQAjkYBBgIwQQYGBACORgEFMDcwNRYvaHR0cHM6Ly93d3cuZmly
bWFwcm9mZXNpb25bbC5jb20vY3BzL3Bkc19lbi5wZGYTAmVuMIIBEgYDVR0gBIIBCTCCAQUwgfcG
CysGAQQB5nkKAQoCMIHnMCBGCCsGAQUFBwIBFiNodHRwOi8vd3d3LmZpcm1heHJvZmVzaW9uYWwu
Y29tL2NwczCB8wYIKwYBBQUHAgIwgeYMgeFDbXN0ZSBlcyB1biBDZX0taWZp Y2FkbyBDb3Jwb3Jh
dGl2byBkZSBTZWxsbyBFbXByZXNhcmlhbCBjdWFsaWZpY2Fkb3MuY3JsMA4GA1UdDwEB/wQEAwIF+DAd
c3RhZG9yIGRlIHNlcnZpY2lvcyBkZSBjb25maWFuemE6IFBhc2VvIGRlIGxhIEJvbmFub3ZhLCA0
NyAgMDgwMTcgQmFyY2Vsb25hMAKGBwQA+xAAQEwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL2Ny
bC5maXJfYXBy2Zlc2lvbmFsLmNvbS9qdWFsaWZpY2Fkb3MuY3JsMA4GA1UdDwEB/wQEAwIF+DAd
BgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwDQYJKoZIhvcNAQELBQADggEBAKYDU8gk5Nu8
9t+Ngb0tYdPfaP31fkA22Qakt5VSPPKbidcf5NZgWN5p/G0MNBkgxu2okYTeeFgMy2GXFGifmtOo3
We9hp8eb7OCSpZnztfGJ4mUXpXqGc6Kly3l+FQXiKEfYmcWiAgNE3NLvdTQN/5BkddMWBCTOAanS
In+xZwyWxHwc9pmyyYRSbgtGJQUy9PECkZgMfnJWxBn5ptlkda3MYGj2pz7Qgq0ny7EdLb3tAxPfj
5ESZOl2ViKDpAWkrnCp60bjZfGnDFnplYP7md9gCrAEumYPEg9se0Qg2F7Olmwib+9+kpss1bUPz
ex7lYm6Dhqh0uI4uU/feMgv9+9qo=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC Firmaprofesional - CUALIFICADOS*

Issuer SERIAL NUMBER: *A62634068*

Issuer OU:	*Certificados Cualificados*
Issuer O:	*Firmaprofesional S.A.*
Issuer C:	*ES*
Subject CN:	*Lleidanetworks Serveis Telemàtics, S.A.*
Subject SERIAL NUMBER:	*A25345331*
Subject OU:	*TECHNICAL DEPARTMENT*
Subject 2.5.4.97:	*VATES-A25345331*
Subject O:	*Lleidanetworks Serveis Telemàtics, S.A.*
Subject ST:	*LLEIDA*
Subject C:	*ES*
Valid from:	*Mon Feb 19 13:37:00 CET 2018*
Valid to:	*Sat Feb 18 13:37:00 CET 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D9:1C:22:66:AB:75:50:8B:2A:67:70:43:2A:F4:02:5F:BC:69:61:63:6F:FB:B2:22:AB:DA:46:13:A2:AA:D1:30:15:AC:CD:0F:0A:9C:58:D8:F0:D4:72:15:D4:B5:C5:C8:E7:63:E7:61:E7:99:78:61:CC:B4:A4:F8:19:CB:67:E8:76:28:0D:F9:B6:C6:81:B2:0E:3F:47:4F:4F:DD:A8:95:38:72:7E:21:B2:12:46:32:59:02:F0:C9:AE:C8:AA:66:A0:A1:9D:2A:18:76:12:85:20:19:AF:6B:2C:36:ED:9B:0E:CC:47:2A:9E:1D:A5:E7:63:31:31:5B:A7:87:AA:40:3F:3D:9D:29:3B:31:C7:79:58:AD:02:9B:46:6D:EC:34:D1:DC:FF:D3:B9:74:BE:6C:8A:3C:14:09:4E:AD:45:B7:B4:22:29:2D:16:20:8F:DE:D8:75:C9:43:59:DB:89:6B:FB:F9:5D:AD:3F:FC:24:5A:60:C9:9D:D5:26:4C:8B:D8:2A:4B:0E:DE:46:60:D0:42:C4:9C:FD:10:ED:9E:99:1B:88:17:03:71:4A:71:8A:1A:E0:FD:0E:84:B9:A2:32:B8:24:12:93:69:1C:FF:88:78:F8:37:8C:5B:76:D6:6F:50:33:D7:F2:AF:CE:9A:07:9F:63:48:C4:70:11:AF:FB:3D:02:03:01:00:01*
Authority Info Access	*http://crl.firmaprofesional.com/cualificados.crt* *http://ocsp.firmaprofesional.com*
Subject Key Identifier	*83:73:0A:37:EB:18:17:66:AA:E7:07:A7:7C:DC:9A:41:C4:B2:AD:46*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.13177.10.1.10.2* *CPS pointer: http://www.firmaprofesional.com/cps* *CPS text: [Éste es un Certificado Corporativo de Sello Empresarial cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]* *Policy OID: 0.4.0.194112.1.1*
CRL Distribution Points	*http://crl.firmaprofesional.com/cualificados.crl*
Extended Key Usage	*id_kp_clientAuth*

Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*CF:14:2F:21:78:F3:FC:04:77:E7:0A:B8:24:38:8D:8D:CB:D9:4E:1C:9D:89:20:DC:EE:BA:57:0B:7E:24:4F:7B*

X509SubjectName

Subject CN:	*Lleidanetworks Serveis Telemàtics, S.A.*
Subject SERIAL NUMBER:	*A25345331*
Subject OU:	*TECHNICAL DEPARTMENT*
Subject 2.5.4.97:	*VATES-A25345331*
Subject O:	*Lleidanetworks Serveis Telemàtics, S.A.*
Subject ST:	*LLEIDA*
Subject C:	*ES*

X509SKI

X509 SK I	*g3MKN+sYF2aq5wenfNyaQcSyrUY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-10-26T01:00:00Z

32.1.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name	*[es]*	*Servicio cualificado de entrega electrónica certificada "Connectaclick"*
Name	*[en]*	*Qualified electronic registered delivery service "Connectaclick"*

Service digital identities

X509SubjectName

Subject CN:	*Lleidanetworks Serveis Telemàtics, S.A.*

Subject SERIAL NUMBER:	*A25345331*
Subject OU:	*TECHNICAL DEPARTMENT*
Subject 2.5.4.97:	*VATES-A25345331*
Subject O:	*Lleidanetworks Serveis Telemàtics, S.A.*
Subject ST:	*LLEIDA*
Subject C:	*ES*

X509SKI

X509 SK I	*g3MKN+sYF2aq5wenfNyaQcSyrUY=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2018-12-26T01:00:00Z*

33 - TSP: BRANDDOCS, S.L.

.

TSP Name

Name	[en]	*BRANDDOCS, S.L.*
Name	[es]	*BRANDDOCS, S.L.*

TSP Trade Name

Name	[en]	*Branddocs SL*
Name	[es]	*Branddocs SL*
Name	[en]	*VATES-B87142618*
Name	[es]	*VATES-B87142618*

PostalAddress

Street Address	[en]	*PASEO CLUB DEPORTIVO NUMERO 1, EDIFICIO 15 A*
Locality	[en]	*POZUELO DE ALARCON*
State Or Province	[en]	*MADRID*
Postal Code	[en]	*28223*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*PASEO CLUB DEPORTIVO NUMERO 1, EDIFICIO 15 A*
Locality	[es]	*POZUELO DE ALARCON*
State Or Province	[es]	*MADRID*
Postal Code	[es]	*28223*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:branddocs@branddocs.com*
URI	[es]	*mailto:branddocs@branddocs.com*
URI	[en]	*http://www.branddocs.solutions/*

TSP Information URI

URI	*[en]*	*http://www.branddocs.solutions/*
URI	*[es]*	*http://www.branddocs.solutions/*

33.1 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals by BRANDDOCS, S.L.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

Service type description	*[en]*	*A preservation service for qualified electronic signatures.*
	[es]	*Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name	*[en]*	*Qualified preservation service for qualified electronic signatures and qualified electronic seals by BRANDDOCS, S.L.*
Name	*[es]*	*Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor BRANDDOCS, S.L.*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *727424342770068517*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJADCCBeigAwIBAgIICbhUle/ILCUwDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQU5BVEFDQSBDQTEgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzIxNDk5MB4X
DTE5MDMxNDE5MjQwMFoXDTIyMDMxMzE5MjQwMFowgZMxCzAJBgNVBAYTAkVTMRUwEwYDVQQKDAxC
cmFuZGRvY3MgU0wxEjAQBgNVBAUTCUI4NzE0MjYxODE/MD0GA1UEAww2U2VydmljaW8gcHJlc2Vy
dmFjacOzbiBkZSBmaXJiYXMgeSBzZWxsb3MgY3VhbGlmaWNhZG9zMRgwFgYDVQRhDA9WQVRFUy1C
ODcxNDI2MTgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDd/8uXdltOPHiT4IBVQHWb
o881QJpzsTD8HMlmuCIXyxy25LrU16SU77qYVZdzu1fA8GCUNBQcxLjhIBCRHX4gWzwDWAaFxmD0
uYwf5uCLAjFPH+rYHFL+sCIOrib91gLvs6wunEFRRDOImmXgszaL7WlBNH9Kt4k45STSIMug9+Ns
5HB6nBdAISDZPyLulWBoYIWIxwWmS8teOBXIDv2nsKBY8K/wsTf6lSBAdgdnt7cfzzBxn6MLE5e6
HBlbW8qBO83rL2FgbShamluRQ3Ym3y+xAPGhEMxxvSuVk85UuY3N2OLbLWIIMB6VRrhB96cV05Qym
9toi4RjUdCPIJQ11AgMBAAGjggMvMIIDKzB8BggrBgEFBQcBAwRwMG4wCAYGBACORgEBMAsGBgQA
jkYBAwIBDzAIBgYEAI5GAQQwNgYGBACORgEFMCwwKhYkaHR0cHM6Ly93d3cudWFuYXRhY2EuY29t
L3B1YmxpYy9jcHMvEwJFTjATBgYEAI5GAQYwCQYHBACORgEGAjCB1wYIKwYBBQUHAQEEgcowgccw
VQYIKwYBBQUHMAKGSWh0dHA6Ly93d3cudWFuYXRhY2EuY29tL3B1YmxpYy9kb3dubG9hZC90c3Bf
Y2VydGlmaWNhdGVzL3N1Ym9yZGluYXRlMS5jcmQwNgYIKwYBBQUHMAGGKmh0dHA6Ly9vY3NwMS51
YW5hdGFjYS5jb20vcHVibGljL3Bra S9vY3NwLzA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AyLnVh
bmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AyMB0GA1UdDgQWBBTKSXuecf8iKnO/4NBB0DbJMskv
pDAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFC1x77BjlX94IMiRH9EEDCBT03IMIGZBgNVHSAE
gZEwgY4wCQYHBACL7EABAzCBgAYLKwYBBAGC8TYBCQYwcTAwBggrBgEFBQcCARYkaHR0cHM6Ly93
d3cudWFuYXRhY2EuY29tL3B1YmxpYy9pLMvMD0GCCsGAQUFBwICMDEMLlF1YWxpZmllZCBjZX0
aWZpY2F0ZSBmb3lgZS1zZWFsIGluIFlbW90ZSBRU0NEMIGPBgNVHR8EgYcwgYQwQKA+oDyGOmh0
dHA6Ly9jcmwxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9DQTFzdWJvcmRpbmFkYS5jcmww
QKA+oDyGOmh0dHA6Ly9jcmwyLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9DQTFzdWJvcmRp
bmFkYS5jcmwwDgYDVR0PAQH/BAQDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDAm
BgNVHREEHzAdgRtjZXI0aWZpY2F0ZXNAYnJhbmQtZG9jcy5jb20wDQYJKoZIhvcNAQELBQADggIB
AHQUsXNJkpM5NTEmPCHJXatvvFkpDo6JZBoGfv7RhQr6Aj2L7seNLlwZ24kEa5Zd6e5nY1bWjLU
Eq2g3MoPXJziEmvl1DNSvKjPhRxtQKF5bHCymYsItrVWie+PTaRG33OFDPfaMbr+lPOVxcKUv4c
RHyxywSemVrnoMb/v2/VCBm0LGEjhWOkAPmFIL1TKUA9nr+gYRVi3s2xIMiWRx0HpKkBvZnILBW
aCREk3usVhpvkb4WmyzWqnRthKPyhVZnxznGDbC7UyN+Qg89EHvMLHHFD+3R40DFWEJPgAweWGqC
QOt775WN9NGSk96AhmXRaA/HaQH1EEg3YNMGzUj6+6SiuYCKyG8HnXSLrTIAAJnJ89kwI3Omlk3
UnC4fxWg5lEHZU3KaO55ce+hWJt9Yjg4sEQjr8PcMeETQlHFhd0Xn2m3FiZ7aTBWhIPC+J48BVU/
zxH+Ey6L53Ufe0umikX40BVWy0cnJO5/qoAg18ChK/cgtu/vQ9QeUWr2966YGYxQZ/y/45P4hXKq
FGu/7jfSZjwYmpvKmwb0b/sUVdu7HDP9QnlYPjF4Dne3goAEzp88Ns8Ik3xiAw3d49TKqnFMxiv9
R9ihrywX3gCBjx+yFB2GIdDDidJlm40M0/NLmgOQbCI8H1E6u3aHDkTwONG103bk1ONpX3yZFc7
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA1 2016*

Issuer OU: *TSP-UANATACA*

Issuer O:	*UANATACA S.A.*
Issuer L:	*Barcelona (see current address at www.uanataca.com/address)*
Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-B87142618*
Subject CN:	*Servicio preservación de firmas y sellos cualificados*
Subject SERIAL NUMBER:	*B87142618*
Subject O:	*Branddocs SL*
Subject C:	*ES*
Valid from:	*Thu Mar 14 20:24:00 CET 2019*
Valid to:	*Sun Mar 13 20:24:00 CET 2022*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DD:FF:CB:97:76:5B:4E:3C:77:D3:E0:80:55:40:75:9B:A3:CF:35:40:9A:73:B1:30:FC:1C:C9:66:B8:22:17:CB:1C:B6:E4:BA:D4:D7:A4:94:EF:BA:98:55:97:73:BB:57:C0:F0:60:94:34:14:1C:C4:B8:E1:94:10:91:1D:7E:20:5B:3C:03:58:06:85:C6:60:F4:B9:8C:08:E6:E0:8B:02:31:4F:1F:E7:D8:1C:52:FE:B0:22:0E:AE:26:FD:D6:02:EF:B3:AC:2E:BC:41:51:44:33:9F:9A:65:E0:B1:E6:8B:ED:69:41:34:7F:4A:B7:89:38:E7:94:FC:24:CB:A0:F7:E3:6C:E4:70:7A:9C:17:40:B5:20:D9:3F:22:EE:95:60:68:60:85:88:C7:05:A6:4B:CB:5E:38:15:E5:0E:FD:A7:B0:A0:58:F2:4F:F0:B1:37:FA:97:90:40:76:07:67:B7:B7:1F:CF:30:71:9F:A3:0B:13:97:BA:1C:18:56:F2:A0:4E:F3:7A:CB:D8:58:1B:4A:16:A6:96:E4:50:DD:89:B7:CB:EC:40:3C:68:44:33:1C:6F:4A:E5:64:F3:95:2E:63:73:76:38:B6:CB:58:82:0C:07:A5:51:AE:10:7D:E9:C5:74:E5:0C:A6:F6:DA:22:E1:18:D4:74:23:E5:25:0D:75:02:03:01:00:01*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15* *id_etsi_qcs_QcSSCD*
Authority Info Access	*http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt* *http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*CA:49:7B:9E:71:FF:22:2A:73:BF:E0:D0:41:D0:36:C9:32:C9:2F:A4*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*
Certificate Policies	*Policy OID: 0.4.0.194112.1.3* *Policy OID: 1.3.6.1.4.1.47286.1.9.6* *CPS pointer: https://www.uanataca.com/public/cps/* *CPS text: [Qualified certificate for e-seal in Remote QSCD]*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl* *http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl*
Extended Key Usage	*id_kp_clientAuth*
Subject Alternative Name	*certificates@brand-docs.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *65:04:C5:1D:4F:9F:6B:E4:C2:6F:AD:85:03:B5:CC:6E:3D:39:E9:40:C7:0B:1F:5E:75:4D:2A:DA:BE:17:66:AC*

X509SubjectName

Subject 2.5.4.97: *VATES-B87142618*

Subject CN: *Servicio preservación de firmas y sellos cualificados*

Subject SERIAL NUMBER: *B87142618*

Subject O: *Branddocs SL*

Subject C: *ES*

X509SKI

X509 SK I *ykl7nnH/Iipzv+DQQdA2yTLJL6Q=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2019-06-24T00:00:00Z

33.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

33.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

34 - TSP: Ecertic Digital Solutions, S.L.

TSP Name

Name	[en]	Ecertic Digital Solutions, S.L.
Name	[es]	Ecertic Digital Solutions, S.L.

TSP Trade Name

Name	[en]	ECERTIC
Name	[es]	ECERTIC
Name	[en]	VATES-B87428728
Name	[es]	VATES-B87428728

PostalAddress

Street Address	[en]	Avda. Europa, 24, Edificio B, Planta 1, Parque Empresarial de La Moraleja
Locality	[en]	Alcobendas
State Or Province	[en]	Madrid
Postal Code	[en]	28108
Country Name	[en]	ES

ElectronicAddress

URI	[en]	mailto:info@ecertic.com
URI	[en]	http://www.ecertic.com

TSP Information URI

URI	[en]	http://www.ecertic.com

34.1 - Service (withdrawn): Qualified timestamps issued by ECERTIC

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name *[en]* *Qualified timestamps issued by ECERTIC*

Name *[es]* *Sellos de tiempo cualificados emitidos por ECERTIC*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *8085602031753677786*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHETCCBPmgAwIBAgIIcDXUNWHay9owDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUys5L1jEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQU5BVEFDQSBDQTIgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzIxNDk5MB4X
DTE5MTAxNzExMzE0N1oXDTI3MTAxNzExMzE0N1owgZcxCzAJBgNVBAYTAkVTMQ8wDQYDVQQHDAZN
QURSSUQxJTAjBgNVBAoMHEVDRVJUSUMgRElHSVRBTCBTT0xVVElPTlMgU0wxFDASBgNVBAsMC0VD
RVJUSUMgVFNQMSAwHgYDVQQDDBdFQ0VSVEIDIFVQUzJRkIFRCBUU1UwMTEYMBYGA1UEYQwPVkFU
RVMtQjg3NDI4NzI4MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxXtC37EsH3Hrpcyt
43aKodB9GpRNST3tH3nWgrODt0LSa3RBXq+IzpG3DK2MnrU4Xs82GanAgIDpCHxOA7Cqa+HBm7Q5a
bApjrYE7gx/LukRO4Beqbi2jKpXPZLCgAyzI1gWbG7fiNdhe02+BDHyu9F7a/3MNX3mWlbTdPmi
JAUY1CwnXLCq6aojcDwOE26tNNMn9kKE6w16Gw37E0sGb06fiC+LEaP/pEweGyzh/DNrwxV6pB2
Z6kuM2WILZu0Ff9EOZWw+5AxpJx6vsoaG8OO1aX8ecQ+H2SW/030t2mEBE4RKfVcuE6R1VKjnz5UC
ZehwwPSvZebLlVckuYZSQIDAQABo4ICPDCCAjgwfgYIKwYBBQUHAQEEcjBwMDYGCCsGAQUFBzAB
hipodHRwOi8vb2NzcDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUHMAGG
Kmh0dHA6Ly9vY3NwMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAdBgNVHQ4EFgQUwRpn
kTj2DCEJD3VGkw1J5cYXZkwCQYDVR0TBAIwADADBgNVHSMEGDAWgBR9V+djgc84HRqmio2jw4RGy
dJEz7CBkwYDVR0gBIGLMIGIMHwGCsGAQQB9yEZAgUwbyA6BggrBgEFBQcCAjAuIDCxIDZXJ0aWZp
Y2FkbyBkZSBzZWxsbyBkZSB0aWVtcG8gZWx1Y3Ryw7NuaWNvLjAwBggrBgEFBQcCARYkaHR0cHM6
Ly93d3cudWFuYXRhY2EuY29tL3B1YmxpYy9jcHMvMAgGBgQAj3oBAjCBjwYDVR0fBIGHMIGEMECg
PqA8hjpodHRwOi8vY3JsMS51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvQ0Eyc3Vib3JkaW5h
ZGEuY3JsMECgPqA8hjpodHRwOi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvQ0Ey
c3Vib3JkaW5hZGEuY3JsMA4GA1UdDwEB/wQEAwIHgDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAb
BgNVHREEFDASgRBpbmZvQGVjZXJ0aWMuY29tMA0GCSqGSIb3DQEBCwUAA4ICAQAxfBJMz2EBVIx2
iz+M8iq+fa983Znu/ohPCyvjvaV7/rltYo+dbMDszbfuwwsPotMGn1wueB3EOr6nWGjEyzQG2q2
0ABhSTTjjmaU/VJNDGuj1/0ykLS/RXk54i+vbQnqVZa9RfYyZVS+WNWYozE3WPggFJIWyqesnHDp7M
LJZ6s9f4MaqU/VrUkQ7tAQYOAtroq2APxumGNK+9WR6nQqg7DISQg6/pPkckTTQVZHoQe7RkhBSkME
0dNbNEqehSZx1RPWW6qvi14Jbz8YX/rlLenmyaFSUiTjxnB8sCcoguHFu+vgc7T8chtRIFru5lLxF
fLH0FMI0ZYuwZv12VG8TqDgHsEx47iaOwnQ8axIZ33TI5ioPwCf94mABKZ3OshZ1D0gHBZqHpSq0
QwDEnOTVFXQ9AA0roB1oo37mSBQA2y28g6Tztc0uqEa0t9pviWWta6Fq0NmB8vmnx2GNOKAMlh
yPW1MSRns7+5YHHboTYswsCxyQdl0cxYSfG20L7SVP9eO8d7Ar3St1tJtdTYoS4BVQ+7ZpdjT
iel3OyMQuHhbbdy2OxIdcS0t87MJuHrd6Vyk4crBSFXmYNXAt4ybDlbvMTy9yZbeECGtHlhvNNWP
8B/6zroTRuJo9lnk1JdKjo9Hc8nZORLazl0yh9FqglUJ6vW5NKCKpsK0T31J2Q==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA2 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B87428728*

Subject CN: *ECERTIC QUALIFIED TSU01*

Subject OU: *ECERTIC TSP*

Subject O: *ECERTIC DIGITAL SOLUTIONS SL*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Thu Oct 17 13:31:47 CEST 2019*

Valid to: *Sun Oct 17 13:31:47 CEST 2027*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:77:C2:DF:B1:2C:1F:71:EB:A5:CC:AD:E3:76:8A:A1:F2:3D:1A:94:4D:49:3D:DF:1F:79:D6:82:B3:83:B7:42:D2:6B:74:41:5E:AF:88:CE:91:B7:0E:4D:8C:C1:4E:17:B3:CD:86:6A:70:20:0E:90:BF:1F:13:80:EC:6A:9A:F8:70:66:ED:0E:5A:6C:0A:63:AD:81:3B:83:1F:CB:BA:44:4E:E0:17:AA:6E:2D:A3:2A:95:CF:64:B0:A0:03:2C:DF:D6:05:9B:1B:B7:E2:35:D8:5E:D3:6F:81:0C:7C:AE:27:D1:7B:6B:FD:CC:35:7D:E6:5A:56:D3:74:F9:A2:24:05:18:D4:2B:78:9D:72:C2:AB:A6:A8:8D:C0:F0:38:4D:BA:B4:D3:4C:9F:D9:0A:13:AC:25:E8:6C:37:EC:4D:2C:19:BD:3A:7E:D0:BE:2C:46:8F:FE:91:30:78:6C:B3:87:F0:CD:AF:0C:55:EA:90:76:67:A9:2E:33:65:88:2D:9B:B4:14:8F:44:41:95:B0:FB:90:31:A4:9C:7A:BE:CA:1A:1B:C3:8E:D5:A5:FC:79:E4:3E:1F:64:96:D3:7D:2D:DA:61:01:13:84:4A:7D:57:2E:13:A4:65:54:A8:E7:CF:95:02:65:E8:70:C1:F3:F9:BD:97:A1:2E:55:5C:92:E6:19:49:02:03:01:00:01*

Authority Info Access

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *C1:1A:67:92:D4:E3:D8:30:84:24:3D:D5:1A:4C:35:27:97:18:5D:99*

Basic Constraints *IsCA: false*

Authority Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Certificate Policies

Policy OID: 1.3.6.1.4.1.47286.2.5

CPS text: [Certificado de sello de tiempo electrónico.]

CPS pointer: https://www.uanataca.com/public/cps/

Policy OID: 0.4.0.2042.1.2

CRL Distribution Points

http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl

http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@ecertic.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0C:74:B1:2B:AE:CE:B8:32:22:44:C2:03:69:CA:00:2F:AE:74:CA:F3:61:5D:C0:FC:9D:C2:4B:39:5E:DC:EC:78*

X509SubjectName

Subject 2.5.4.97: *VATES-B87428728*

Subject CN: *ECERTIC QUALIFIED TSU01*

Subject OU: *ECERTIC TSP*

Subject O: *ECERTIC DIGITAL SOLUTIONS SL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *wRpnktTj2DCEJD3VGkw1J5cYXZk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-10-26T01:00:00Z*

34.1.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Qualified timestamps issued by ECERTIC*

Name *[es]* *Sellos de tiempo cualificados emitidos por ECERTIC*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B87428728*

Subject CN: *ECERTIC QUALIFIED TSU01*

Subject OU: *ECERTIC TSP*

Subject O: *ECERTIC DIGITAL SOLUTIONS SL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *wRpnktTj2DCEJD3VGkw1J5cYXZk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-11-06T01:00:00Z*

35 - TSP: DIGITEL ON TRUSTED SERVICES S.L.U.

.

TSP Name

Name	*[es]*	*DIGITEL ON TRUSTED SERVICES S.L.U.*
Name	*[en]*	*DIGITEL ON TRUSTED SERVICES S.L.U.*

TSP Trade Name

Name	*[es]*	*DIGITEL ON TRUSTED SERVICES*
Name	*[en]*	*DIGITEL ON TRUSTED SERVICES*
Name	*[en]*	*VATES-B47447560*
Name	*[en]*	*DIGITEL ON TRUSTED SERVICES SLU*

PostalAddress

Street Address	*[es]*	*C/ ENRIQUE CUBERO, 9*
Locality	*[es]*	*VALLADOLID*
State Or Province	*[es]*	*VALLADOLID*
Postal Code	*[es]*	*47014*
Country Name	*[es]*	*ES*

PostalAddress

Street Address	*[en]*	*C/ ENRIQUE CUBERO 9*
Locality	*[en]*	*VALLADOLID*
State Or Province	*[en]*	*VALLADOLID*
Postal Code	*[en]*	*47014*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[es]*	*mailto:contratacion@madisonmk.com*
URI	*[es]*	*https://www.digitelts.es*
URI	*[en]*	*https://www.digitelts.es*

URI	*[en]*	*mailto:contratacion@madisonmk.com*

TSP Information URI

URI	*[es]*	*https://www.digitelts.es*
URI	*[en]*	*https://www.digitelts.es*

35.1 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[es]*	*Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES*
Name	*[en]*	*Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *112872936999496967491 3*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIbTCCB1WgAwIBAgIJPTBERb70mvShMA0GCSqGSIb3DQEBCwUAMIIBBDELMAkGA1UEBhMCRVMx
DzANBgNVBAgMBk1BRFIJRDEPMA0GA1UEBwwGTUFET1klEMUIwQAYDVQQLDDIzZWUgY3VycmVudCBh
ZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxITAfBgNVBAsMGEFD
IENBTUVSRkISTUEgVFNBICI0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRF
Uy1BODI3NDMyODExGzAZBgNVBAoMEkFDIENBTUVSRkISTUEgUy5BLjEhMB8GA1UEAwwYQUMgQ0FN
RVJGSVJNQSBUU0EgLSAyMDE2MB4XDTE5MDgyMzExMTMxNi1oxDTI0MDgyMTExMTMxNi1owdzEkMCIG
A1UEAwwbREIHSVRFTCBPTiBUUlVTVEVEIFNFUlZJQ0VTMRgwFgYDVQRhDA9WQVRFUy1CNDc0NDc1
NjAxKDAmBgNVBAoMH0RJR0lURUwgT04gVFJVU1RFRCBTRVJWSUNFUyBTTFUxCzAJBgNVBAYTAkVT
MIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnOqyzwoIZ9RWJKhng/XN+LNkO6cCKK4Og
7QC8PH9lUnybskNGpC3BYKAfNVIBUl6ZMVHVgCDJfs161PHQxEFz8WsysHzNVYhLrUvUIlLZuf
dYqHh/kR5uGlcx6BCO+jegsuhmDrvqdAtZLjThu1cFRe34MXciP5mYaoNlHWtOAfyldb0RgyJFvG
mQn4VJ3bOd6SCTjD3+sNp2bxdRMJprLScfbZgPpmmajrBgOnRMsD5f4NsoRgAmhm/7UT6UzJf6kY
ET6pKIrTNmlgxXVRv1Wq3kNCU4u77lQT3NE9PmOxWsMbV9zI/OPp0H4xNQTogm15NUsrAGjIDOMi
navxxQIDAQABo4IEazCCB6cwDAYDVR0TAQH/BAIwADAOBgNVHQ8BAh8EBAMCBkAwFgYDVR0lAQH/
BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFPWAs2+j+jlEVE8Tx2HvBvC1zNbbMH4GCCsGAQUFBwEB
BHIwcDBGBggrBgEFBQcwAoY6aHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9hY19jYW1l
cmZpcm1hX3RzYS0yMDE2LmNydDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3AuY2FtZXJmaXJhYS5j
b20wggFFBgNVHSMEggE8MIIBOIAUHm21xj/vkIVeNrib/RCquik7TyhygcUJpIIBEDCCAQwxCzAJ
BgNVBAYTAkVTMQ8wDQYDVQQIDAZNQURSSUQxDzANBgNVBAcMBk1BRFIJRDE6MDgGA1UECwwxe2Vl
IGN1cnJlbnQgYWRkcmVzcyBhdCB3d3cuY2FtZXJmaXJhYS5jb20vYWRkcmVzczEpMCcGA1UECwwg
Q0hBTUFUIlMgT0YgQ09NTUVSQ0UgUk9PVCAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0MzI4NzEYMBYG
A1UEYQwPVkFURVMtQTgyNzQzMjg3MRswGQYDVQQKDBJBQyBDQU1FUkZJUk1BIFMuQS4xKTAnBgNV
BAMMIENIQU1CRVTTIE9GIENPTUlTUFUkNFI5PTIQgLSAyMDE2ggeVt6WKVP8GjtCBggYDYR0IBH5w
eTA6oDigNoY0aHR0cDovL2NybC5jYW1lcmZpcm1hLmNvbS9bY19jYW1lcmZpcm1hX3RzYS0yMDE2
LmNybDA7oDmgN4Y1aHR0cDovL2NybDEuY2FtZXJmaXJhYS5jb20vYWNlY2FtZXJmaXJhYV90e2Ei
MjAxNi5jcmwwHAYDVR0SBBUwE4ERY2FAY2FtZXJmaXJhYS5jb20wgcYGA1UdIASBvjCBuzCBrQYN
KwYBBAGBby4KEAUBATCBmzApBggrBgEFBQcCARYdaHR0cHM6Ly9wb2spY3kuY2FtZXJmaXJhYS5j
b20wbgYIKwYBBQUHAgIwYgxgQ2VydGlmaWNhZG8gQ3VhbGlmaWNhZG8gZGUgVFNVLtBDb25zdWx0
ZSBsYXMgY29uZGljaW9uZXMgZGUgdXNvIGVulGh0dHBzOi8vcG9saWN5LmNhbWVyZmlybWEuY29t
MAkGBwQAi+xAAQMwgdoGCCsGAQUFBwEDBIHNMIHKMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wCAYG
BACORgEEMIGRBgYEAI5GAQUwgYYwQRY7aHR0cHM6Ly9wZHBuY2FtZXJmaXJhYS5jb20vZG9jcy9Q
RFNfTGVnYWxfUGVyc29uLXYxLjBFTi5wZGYTAmVuMEEWO2h0dHBzOi8vcGRzLmNhbWVyZmlybWEu
Y29tL2RvY3MvUERTX0xlZ2FsX1BlcnNvbi1ZMS4wRVMucGRmEwJlczATBgYEAI5GAQYwCQYHBACO
RgEGAjANBgkqhkiG9w0BAQsFAAOCAgEAKu1m/d6yNn4PR2wKvkTdqBxqfwr6p4q4JjoSwo7DZnck
Dn4hwZXuUHtEVVjjQmw6CHuKzZ5COnRQrnbCR31XUEsF5jmB9rzA5TfXfinrCQRL6mzXCYzhN1
mnqtLTnio7Bo1xZxlh1IaJqI0Vo9BR9/g9BtDZ9/To6qGHLXRKwS8peVJnu49LuOErUe6bEMImbk
p9gWCTPJuzuPN63pKmfU1QNhaqlj+7RT3J1vVZub+3iO9G2XS/cNb3YbENJUlzKESTX94aeADPcA
CGjypCIXi/WIVaZ8VRpMFDFbVg4E48Pby8KmlF1VZstxCOsIvOIiAJdyWzPMSNbulaEwJv52QUG
uCjg0Rp7Ue7+bVF1T4dqd6/pUu/K/dB/ZJg7UnHkqOcWVcynLI0ECjuEwkLgIUQbNTue4P4foC
bKKLvyGN4yIlb++OHDagtySTDNiILdGPHcANIMCTQpkkmQnbSyRZaEhmXcgz9Iw+Su7SuzN6PU0
G8FFih87gKy8+V0tA5+WADknOtpR2A6tP/q7pqJmNZY0ZCJQ65uZAUoICzldyc5gAj3JOHn/1Z3
aFKt2LVg2IhfyTX0M9458QSKP8REeeawQu3SvfbC0s5HBAb0WtjMBDG0y8PVzOb0EMu4hPflacal
Lx8F4N/BbqGUkp+lqnwuNKjolzte/uE=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*AC CAMERFIRMA TSA - 2016*
Issuer O:	*AC CAMERFIRMA S.A.*
Issuer 2.5.4.97:	*VATES-A82743287*

Issuer SERIAL NUMBER:	*A82743287*
Issuer OU:	*AC CAMERFIRMA TSA - 2016*
Issuer OU:	*see current address at https://www.camerfirma.com/address*
Issuer L:	*MADRID*
Issuer ST:	*MADRID*
Issuer C:	*ES*
Subject C:	*ES*
Subject O:	*DIGITEL ON TRUSTED SERVICES SLU*
Subject 2.5.4.97:	*VATES-B47447560*
Subject CN:	*DIGITEL ON TRUSTED SERVICES*
Valid from:	*Fri Aug 23 13:13:17 CEST 2019*
Valid to:	*Wed Aug 21 13:13:17 CEST 2024*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:EA:AF:CF:0A:08:67:D4:56:24:A6:E7:83:F5:CD:F8:B3:64:3B:A0:8A:2B:83:A0:ED:00:91:3C:7F:56:52:7C:A1:22:C9:0D:1A:90:B7:05:82:B8:35:57:C8:F1:4E:9F:64:C5:47:56:00:83:7C:8B:C9:EB:53:C7:43:11:05:AF:C5:AE:B3:21:F3:34:D6:21:2E:B5:2F:50:8D:49:2D:9B:9F:75:8A:87:87:F9:11:E6:E1:B4:73:1E:81:08:EF:A3:7A:0B:2E:86:60:EB:BE:A7:40:B5:92:E3:4E:1B:B5:70:54:5E:DF:83:17:72:23:F9:99:86:A8:36:51:D6:B4:E0:1F:CA:57:5B:D1:18:32:24:5B:C6:99:09:F8:54:9D:E1:39:DE:92:09:38:C3:DF:EB:0D:A7:66:F1:75:13:09:A6:B2:D2:71:F6:D9:80:FA:66:99:A8:EB:06:03:A7:44:CB:03:E5:FE:0D:B2:84:60:02:68:66:FF:B5:13:E9:4C:C9:7E:89:18:11:3E:A9:28:8B:53:36:69:60:C5:75:51:BF:55:AA:DE:43:42:53:8B:BB:EE:54:13:DC:D1:3D:3E:63:B1:5A:C3:21:57:DC:C8:FC:E3:E9:D0:7E:31:35:04:E8:AA:6D:79:35:4B:2B:00:62:65:0C:E3:22:9D:AB:F1:C5:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*F5:80:B3:6F:A3:FA:39:44:54:4F:13:C7:61:EF:06:F0:88:CC:D6:E1*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma_tsa-2016.crt* *http://ocsp.camerfirma.com*
Authority Key Identifier	*1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma_tsa-2016.crl* *http://crl1.camerfirma.com/ac_camerfirma_tsa-2016.crl*
Issuer Alternative Name	*ca@camerfirma.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.17326.10.16.5.1.1* *CPS pointer: https://policy.camerfirma.com* *CPS text: [Certificado Cualificado de TSU. Consulte las condiciones de uso en https://policy.camerfirma.com]* *Policy OID: 0.4.0.194112.1.3*

QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B9:90:57:F8:85:AD:50:70:55:A0:34:D0:29:5C:12:CD:E9:10:EA:47:51:61:51:18:DC:E2:9A:81:4F:AB:B0:FA*

X509SubjectName

Subject C:	*ES*
Subject O:	*DIGITEL ON TRUSTED SERVICES SLU*
Subject 2.5.4.97:	*VATES-B47447560*
Subject CN:	*DIGITEL ON TRUSTED SERVICES*

X509SKI

X509 SK I	*9YCzb6P6OURUTxPHYe8G8IjM1uE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2019-12-16T01:00:00Z

35.2 - Service (granted): Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES 2020*

Service digital identities

Certificate fields details

Version:	*3*

Serial Number: *870476239836202459339*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIRTCCBi2gAwIBAgIULzBI2CZ2lODLMA0GCSqGSIb3DQEBCwUAMIIBBDELMAkGA1UEBhMCRVMx
DzANBgNVBAgMBk1BRFJJRDEPMA0GA1UEBwwGTUFEUklEMUIwQAYDVQQLDDlzZWUgY3VycmVudCBh
ZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxITAfBgNVBAsMGEFD
IENBTUVSRkJSTUEgVFNBICA0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRF
Uy1B0DI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkJSTUEgUy5BLjEbMB8GA1UEAwwYQUMgQ0FN
RVJGSVJNQSBUU0EgLSAyMDE2MbHXDTIwMDUyNzE2MzQxNFoXDTI1MDUyNjE2MzQxNFowdzEkMCIG
A1UEAwwbRElHSVRFTCBPTiBUUlVTVEVEIFNFUlZJQ0VTMRgwFgYDVQRhDA9WQVRFUy1CNDc0NDc1
NjAxKDAmBgNVBAoMH0RJ0lURUwgT04gVFJVU1RFRCBTRVJWSUNFUyBTTFUxCzAJBgNVBAYTAkVT
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx2cMcdWg4PpmoCLQYpp9mlRBL6lQ5TNY
WTFFB60f+OsrLBRHVTqTe6dfUfxfcOJfKzLKACXqyr4UWaouQFr8GBQ7HsZI5DYrWHT06XqBkSif
/d+NaBtfiQ37FP0b0sYPRMMfYLFRoMEYB5orFi3tXhGSXpcPQKryh/Ktbps0ulN03DR6YQtyEuR5P
fGPTFk8+rNxWDaR4BbnZKj+oOMKlfeR3Zz2f10vTr1/RnKtP/33AcGmiwOGjr5RWQrnSS5ZrSag
mcwE5+gM2aqkgPFV6nV/FMV+AS0agDp19xHsDK3Sy17MX0EkLUlhgUMwroJGsyKnMp+CAIU8YgIR
tgrYQIDAQABo4IDQzCCAzBwIDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBkAwFgYDVR0lAQH/
BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFNFOEArQT/xxtpEdG4PHoTvUjgYyeMH4GCCsGAQUFBwEB
BHIwcDBGBggrBgEFBQcwAoY6aHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9hY19jYW1l
cmZpcm1hX3RzYS0yMDE2LmNydDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3AuY2FiZXJmaXJtYS5j
h20wHwYDVR0jBBgwFoAUHm21xjvklVGNrfbRCqutk7TwwgYIGA1UdIwR7MHkwOqA6oDaGNGh0
dHA6Ly9jcmwuY2FiZXJmaXJtYS5jb20vYWNlY2FiZXJmaXJtYV90c2EtMjAxNi5jcmwwO6A5oDeG
NWh0dHA6Ly9jcmwxLmNhbWVyZmlybWEuY29tL2FjX2NhbWVyZmlybWFfdHNhL1wMTYuY3JsMBwG
A1UdEgQVMBOBEWNhQGNhbWVyZmlybWEuY29tMIIHGBgNVHSAEgb4wgbswga0GDSsGAQQBg5cuChAF
AQEwgZswKQYIKwYBBQUHAgEWHWhdHBzOi8vcG9saWNSLmNhbWVyZmlybWEuY29tMG4GCCsGAQUF
BwICMGIMYFNlcnRpZmlj YWRvIEN1YWxpZmlj YWRvIGRlIFRTVS4gQ29uc3VsdGUgbGFzIGNvbmRp
Y2lvbmVzIGRlIHVzbyBlbiBodHRwczovL3BvbGljeS5jYW1lcmZpcm1hLmNvbTAJBgcEAIvsQAED
MIHaBggrBgEFBQcBAwSBzTCByjAIBgYEAI5GAQEwCwYGBACORgEDAgEPMAgGBgQAjkYBBDCBkQYG
BACORgEFMIGGMEEWO2hddHBzOi8vcGRzLmNhbWVyZmlybWEuY29tL2Rcy3Mvi1ERTX0tZZFsX1Bl
cnNvbi2MS4wRU4uGRmEwJlbyBBFjIodHRwczovL3Bkcy5jYW1lcmZpcm1hLmNvbS9kb2NzL1BE
U19MZWdhbF9QZXJzb24tdjEuMEVTLnBkZhMCZXMwEwYGBACORgEGMAkGBwQAjkYBBghwDQYJKoZI
hvcNAQELBQADggIBAEBXATHtPSZoY1xS9smcWRc+KQ0HndFc2XnskMgIRfxTI+xuaYbbVmTOnof4
7vS73CEvE8BPU9RA9d7ZXcW0B6EUNraIAD25HpzBV57DFmHzFYy9wBn5ezIX3mMA4QNmvqyNUm
AmfXvx8ptAV4UU8TzoWwu6m8/0lTUOh72YafIZpnVFEzQjlWTkvTrH5OadUlloAvoO69mbktpcOwl
naDnhR5pNZ1QI933HsjrPeOnlR3/UnrS2cukOygymylWHGP49TYaz7CBh4MMrKITszr5lVnXcjks
AmXOq4lRP9IE2kwOLXzOxLbOf4MEiYyju/2seFRlGB4tPk+L36JpnXf6kZc9NOz3L9gHTpsq/7ZO
udErfB9NENcZzpqTAvXHFldIZ6tob4zmMcVMgoN/BsZ8+OzjNKcC1kK4GedHkP33G63lWyt3Q6Z
bFgmTG3CaxUiZdTW7Ya7UZHt9VgpO9R8FoBPsS/k+1GcNsdAfsD0vNTYw1TgZEWqreo+MsKx2c8
8NX70O66nR9ErRjYgr4AnrxnJnlaz17kxQGyxtZq28X1dOHqLK3jUDN7c8sTOsBs3NbDZwhyfCK9
Ec+gtPXcjXcW5xzeSZsB2oKjL+9OI7Cx2RBuK3tVmd44lH4swzilt/bazP7Dz35RdyPwJrf59G86
LcVvV1vhaq4JjsqP

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *AC CAMERFIRMA TSA - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *AC CAMERFIRMA TSA - 2016*

Issuer OU: *see current address at https://www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject C: *ES*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject CN: *DIGITEL ON TRUSTED SERVICES*

Valid from: *Wed May 27 18:34:14 CEST 2020*

Valid to: *Mon May 26 18:34:14 CEST 2025*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:67:0C:71:D5:A0:E0:FA:66:A0:22:D0:62:9A:7D:9A:54:61:2F:A9:50:E5:33:58:59:31:45:07:AD:1F:F8:EB:2B:2C:14:47:55:3A:93:7B:A7:54:7E:F7:DC:38:9B:45:2A:B2:CA:00:25:EA:CA:BE:09:59:AA:1A:40:5A:FC:18:14:3B:1E:C6:48:E4:36:2B:58:74:F4:E9:78:01:B1:28:9F:FD:DF:8D:68:17:EB:43:7E:C5:3F:46:F4:B1:83:D1:30:C7:D8:2C:54:68:30:46:01:E6:8A:C5:8B:7B:57:84:64:97:A5:C3:D0:2A:BC:A1:FC:AB:5B:A6:CD:2E:94:DD:37:0D:1E:98:42:DC:84:B9:1E:4F:7C:63:D3:16:4F:3E:AC:DC:56:0D:A4:78:05:B9:D9:2A:3F:A8:38:C2:A5:7D:E4:77:67:3D:9F:D7:4B:D3:AF:5F:D1:9C:A8:AD:3F:FD:F7:01:E1:A6:8B:03:86:8E:BE:51:59:0A:E7:49:2E:59:AD:26:A0:99:CC:04:E7:E8:0C:D9:AA:A4:80:F1:55:EA:75:7F:14:C5:7E:01:2D:1A:80:3A:75:F6:C1:EC:0C:AD:D2:C8:8E:CC:5F:41:24:2D:49:61:81:43:30:AE:82:46:B3:22:A7:32:9F:82:00:85:3C:62:02:11:B6:0A:E2:61:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*D1:4E:10:0A:D0:4F:FC:71:B6:91:1D:1B:83:C7:A1:3B:D4:81:8C:9E*
Authority Info Access	*http://www.camerfirma.com/certs/ac_camerfirma_tsa-2016.crt* *http://ocsp.camerfirma.com*
Authority Key Identifier	*1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C*
CRL Distribution Points	*http://crl.camerfirma.com/ac_camerfirma_tsa-2016.crl* *http://crl1.camerfirma.com/ac_camerfirma_tsa-2016.crl*
Issuer Alternative Name	*ca@camerfirma.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.17326.10.16.5.1.1* *CPS pointer: https://policy.camerfirma.com* *CPS text: [Certificado Cualificado de TSU. Consulte las condiciones de uso en https://policy.camerfirma.com]* *Policy OID: 0.4.0.194112.1.3*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D1:A9:E8:21:8D:8D:4C:33:3F:41:F3:0F:7F:03:0B:39:5F:F8:C6:5C:8E:88:07:1F:DE:09:0B:CF:63:40:21:BF*

X509SubjectName

Subject C:	*ES*
Subject O:	*DIGITEL ON TRUSTED SERVICES SLU*
Subject 2.5.4.97:	*VATES-B47447560*
Subject CN:	*DIGITEL ON TRUSTED SERVICES*

X509SKI

X509 SK I	*0U4QCtBP/HG2kR0bg8ehO9SBjJ4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2021-02-25T01:00:00Z*

36 - TSP: VIAFIRMA, S.L.

.

TSP Name

Name	[es]	*VIAFIRMA, S.L.*
Name	[en]	*VIAFIRMA, S.L.*

TSP Trade Name

Name	[en]	*VIAFIRMA*
Name	[en]	*VATES-B91052142*
Name	[en]	*VIAFIRMA SOCIEDAD LIMITADA*

PostalAddress

Street Address	[en]	*Glorieta Fernando Quiñones, S/N. Edificio CENTRIS, planta baja, módulo 8.*
Locality	[en]	*Tomares*
State Or Province	[en]	*Sevilla*
Postal Code	[en]	*41940*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*Glorieta Fernando Quiñones, S/N. Edificio CENTRIS, planta baja, módulo 8.*
Locality	[es]	*Tomares*
State Or Province	[es]	*Sevilla*
Postal Code	[es]	*41940*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:psc@viafirma.com*
URI	[en]	*https://qtsp.viafirma.com*

TSP Information URI

URI	[en]	*https://qtsp.viafirma.com*

36.1 - Service (granted): Sellos de tiempo cualificados emitidos por VIAFIRMATSA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos de tiempo cualificados emitidos por VIAFIRMATSA*

Name *[en]* *Qualified timestamps issued by VIAFIRMATSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *327191426851532438764718424645512795330867118978*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGWTCCBEGgAwIBAgIUOU/FYMDvOMPpbeRLvkLZ/9jEQ4IwDQYJKoZIhvcNAQELBQAwgYIxCzAJ
BgNVBAYTAkVTMSMwIQYDVQQKDBpWSUFGSVJNQSBTT0NJRURBRCBMSU1JVEFEQTEWMBQGA1UECwwN
VklBRkISTUEgUVRTUDEYMBYGA1UEBRMPVkFURVMtQjkxMDUyMTQyMRwwGgYDVQQDDBNWSUFGSVJN
QSBIU0EgU1VCIENlBMB4XDTE5MTAxNzEyMzUzOVoXDTI0MTAxNzEyMzUzOVowezELMAkGA1UEBhMC
RVMxIzAhBgNVBAoMGlZIQUZlUk1BIFNPQ0lFREFEIEsJTUlUQURBMRYwFAYDVQQLDA1WSUFGSVJN
QSBRVFNQMRUwEwYDVQQDDAxWSUFGSVJNQSBUU0ExGDAWBgNVBGEMD1ZBVEVTLUI5MTA1MjE0MjCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANBhf61JDRVD7tA5GfPMzqOwrYz9uNaiEXT
JegDNBSR3FJd2YY+QKwTOqzo9lOlZA4eKaQVw3C/5Io3GgS/ikgDXgfjlNPageIXfLEDBQMCCg69
8BDtQSTmPS6swujtZDl2tQ7UWpZ0uNNN/sOgH0Inqr+gg2OxNwAzGYbz9c8DmVONdj9k6VHl7n5e
EgNH+WolJuxDfV+73Dw6sLQIAe85Wwr8SeV7iVrUk9MDvC5uzwmbg08hkS/OT/NBla13vrPm2QGw
LbuLsOtuxmQdd48WawbP1e/rJGriIeIRdbb/kp4/upmpVNS/cB1q3s6mlmEszze1iX3WJ5f61MrnN
6tMCAwEAAaOCAcswggHHMG0GCCsGAQUFBwEBBGEwXzAyBggrBgEFBQcwAoYmaHR0cDovL3F0c3Au
dmlhZmlybWEuY29tL3RzcC9zdWJjYS5jcnQwKQYIKwYBBQUHMAGGHWh0dHA6Ly9xdHNwLnZpYWZp
cmlhLmNvbS9vY3NwMB0GA1UdDgQWBBRKVUjKFLDUpDmEb9Oqa8ZFse0fwDAMBgNVHRMBAf8EAjAA
MB8GA1UdIwQYMBaAFErIAgQYQ8K9fwOQuU3E8jcvr4mMCsGA1UdEAQkMCKADzIwMTkxMDE3MTIz
NTM5WoEPMjAyMjEwMTcxMjM1MzlaMEMGA1UdIAQ8MDowOAYKKwYBBAGC300HAzAqMCgGCCsGAQUF
BwIBFhxodHRwOn8vcXRzcC52aWFmaXhYS5jb20vY3BzMGHGA1UdHwRnMGUwMKAuoCyGKmh0dHA6
Ly9xdHNwLnZpYWZpcm1hLmNvbS90c3AvdHNhX3N1YmNhLmNybDAxoC+gLYYraHR0cDovL3F0c3Ax
LnZpYWZpcm1hLmNvbS90c3AvdHNhX3N1YmNhLmNybDAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/
BAwwCgYIKwYBBQUHAwgwDQYJKoZIhvcNAQELBQADggIBAJVixpzt0dVY1Ni07WDqUc+meoKxQVARz
rJ5QJ4vnYi0unKwFaEpz6tFÚXTGkY+zoR6622STqrv+P6tnKp6qAqqQU70KIuqUEIE59VqyPJ+34R
5f9IK9vaE3NvD76z7HSE9uQBD6/X5ePwWR67Nj3YUi4VhmoqV34VSrhIgp0fXQttCMk93uUjagTm
t8UcRU5RSUZTPI1F45VjkkqSKjM/5C1ob27xbmc8R3pSkmtI6aIY6VnehNO65xNvBKv7ACmTiYT/
E+7g7uiNo1epYGjPsLwJ66llhhxjT5p2pX6Snq0mJKIiYQc5M9Z+u8iennElcA0X3KsWGZ2BY
ujanF3V4k2+85jR2HU/tE0R+rKA/xOu3qrfotb9xZBCgFFnL8TRUrXs3KlcCaU/YGalNzyqsb++m8
Wvck7qyxHNAvOJm/NB+rvkwJJL+7nG+UQWzjlkqF4AkX3T2U6ViRUPyM/ppatLulrfW1QMAQBx+C
GqKylBe6eKQvFKvYr821y3q8rZ1c20lPi9oT/x/csrj3VHOIXcJvaV24URbKr3ko/HpykyTy9LU
A7lyiJpCPQggfbCy+01nHVwUZ77ivqi15sBRvf9XQsQ9G/58szWpQnoE9QadkEYgpCulvsv43c/J
J+WMNA5zIKyyYpV91E7kgssMfQQr82Rf7gD0/IWZ3VIF

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *VIAFIRMA TSA SUB CA*

Issuer SERIAL NUMBER: *VATES-B91052142*

Issuer OU: *VIAFIRMA QTSP*

Issuer O: *VIAFIRMA SOCIEDAD LIMITADA*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B91052142*

Subject CN: *VIAFIRMA TSA*

Subject OU: *VIAFIRMA QTSP*

Subject O: *VIAFIRMA SOCIEDAD LIMITADA*

Subject C: *ES*

Valid from: *Thu Oct 17 14:35:39 CEST 2019*

Valid to: *Thu Oct 17 14:35:39 CEST 2024*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D0:61:7F:AD:75:24:34:55:0F:BB:40:E4:67:CF:33:3A:8E:C1:F6:33:F6:E3:5A:88:45:D3:25:E8:03:34:14:91:DC:52:5D:D9:86:3E:40:AC:13:3A:AC:E8:F4:93:A5:64:0E:1E:29:A4:15:C3:70:BF:E4:8A:37:1A:04:BF:8A:48:0E:5E:02:23:94:D3:DA:81:E2:57:7C:B1:03:05:03:02:0A:AE:BD:F0:10:ED:41:24:E6:3D:2E:AC:C2:E8:DF:64:39:76:B5:0E:D4:5A:96:74:B8:D3:4D:FE:C3:A0:1F:42:2B:AA:BF:A0:83:63:B1:37:00:33:19:86:F3:F5:CF:03:99:53:8D:76:3F:64:E9:51:E5:EE:7E:5E:12:03:47:F9:6A:25:26:EC:43:7D:5F:BB:DC:3C:3A:B0:B4:09:01:EF:39:5B:0A:FC:49:E5:7B:89:5A:D4:93:D3:03:BC:2E:6E:CF:09:9B:83:4F:21:91:2F:CE:4F:F3:41:95:AD:77:BE:B3:E6:D9:01:B0:2D:BB:8B:B0:EB:6E:C6:64:1D:77:8F:16:6B:06:CF:D5:EF:EB:24:6A:E2:21:E7:D1:75:B6:FF:92:9E:3F:BA:99:A9:54:D4:BF:70:1D:6A:DE:CE:A6:96:61:2C:CD:ED:62:5F:75:89:E5:FE:B5:32:BA:0D:EA:23:02:03:01:00:01*

Authority Info Access

http://qtsp.viafirma.com/tsp/subca.crt

http://qtsp.viafirma.com/ocsp

Subject Key Identifier *4A:55:48:CA:14:B0:D4:A4:39:84:6F:D3:AA:6B:C6:45:B1:ED:1F:C0*

Basic Constraints *IsCA: false*

Authority Key Identifier *4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26*

Certificate Policies

Policy OID: 1.3.6.1.4.1.34253.7.3

CPS pointer: http://qtsp.viafirma.com/cps

CRL Distribution Points

http://qtsp.viafirma.com/tsp/tsa_subca.crl

http://qtsp1.viafirma.com/tsp/tsa_subca.crl

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *84:7E:85:86:E8:42:BD:34:C7:F5:30:8B:9C:28:73:E5:45:BE:79:CA:80:53:7F:E7:BC:6A:2C:A5:C8:26:B0:26*

X509SubjectName

Subject 2.5.4.97: *VATES-B91052142*

Subject CN: *VIAFIRMA TSA*

Subject OU: *VIAFIRMA QTSP*

Subject O: *VIAFIRMA SOCIEDAD LIMITADA*

Subject C: *ES*

X509SKI

X509 SK I *SlVIyhSw1KQ5hG/TqmvGRbHtH8A=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2020-04-28T00:00:00Z

37 - TSP: VALIDATED ID, S.L

.

TSP Name

Name	[es]	*VALIDATED ID, S.L*
Name	[en]	*VALIDATED ID, S.L*

TSP Trade Name

Name	[en]	*VALIDATED ID SL*
Name	[en]	*VATES-B65750721*

PostalAddress

Street Address	[en]	*C/ Aragó, nº179 planta 4*
Locality	[en]	*BARCELONA*
State Or Province	[en]	*BARCELONA*
Postal Code	[en]	*08011*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*C/ Aragó, nº179 planta 4*
Locality	[es]	*BARCELONA*
State Or Province	[es]	*BARCELONA*
Postal Code	[es]	*08011*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:admin@validatedid.com*
URI	[en]	*https://validatedid.com*

TSP Information URI

URI	[en]	*validatedid.com*

37.1 - Service (granted): Sellos de tiempo cualificados emitidos por VALIDATED ID

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos de tiempo cualificados emitidos por VALIDATED ID*

Name *[en]* *Qualified timestamps issued by VALIDATED ID*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7427016217577742020*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHFDCCBPygAwIBAgIIZxIP5I3JXsQwDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUyc5B1jEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRonGAYDVQQDDBFVQUSBVEFDQSBDQTIgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzIzNDk5MB4X
DTE5MTEyNjE3NDUxMVoXDTI3MTEyNjE3NDUxMVowgZcxCzAJBgNVBAYTAkVTMRIwEAYDVQQHDAIC
QVJDRUxPTkExGDAWBgNVBAoMD1ZBTEIEQVRFRCBJRCBTTDEZMBcGA1UECwwQVkFMSURBVEVEIEIE
IFRTUDEIMCMGA1UEAwwcVkFMSURBVEVEIEIEIFFVQUxJRkIFRCBUU1UwMTEYMBYGA1UEYQwPVkFU
RVMtQY1NzUwNzIxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyvHY6jyVcCONjRmu
Lxfq6TXkRq2tpGJeOy7W9AVrdCMGib9ETCrPUyQUwIrfVgXWeBKdg0xkt2r+x0120MmH1tHiuEzmJ
bc0pQyrW17q2rEbiKW0DqxTv/MHgmT0aJie5oC99PisVWxKD8dWznElmZCdxJRIC7d+1NHrPAEVe
lSut4xVoo7X1xEjvmaB4Kya06J+vp7yJR1g4X+NVxACeI8LciRxpo9TAFiqy76Xnvq+URpU0dI56
jtMpvUNsNMw286r+e2VwAJUu/qkw1ajIc/wp9/4vfx6p3fNBTFwwV3PX33r3FJTYSvq4sX5Cz9
mQFJzD0w3oX2+RIdctILGwIDAQABo4ICPzCCAjswfgYIKwYBBQUHAQEEcjBwMDYGCCsGAQUFBzAB
hipodHRwOi8vb2NzcDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUHMAGG
Kmh0dlA6Ly9vY3NwMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAdBgNVHQ4EFgQU6FFO
3bzMcJwRNvbzytY4bhYnpcwCQYDVR0TBAIwADAfBgNVHSMEGDAWgBR9V+dgc84HRqmo2jw4RGy
dJIz/TCBkwYDVR0gBIGLMIGIMIHwCCsGAQQB8gYE2AgUwbjA6BggrBgEFBQcCAjAuDCxDZXJ0aWZp
Y2FkbyBkZSBzZWxsbyBkZSB0aWVtcG8gZWx1Y3Ryw7Nua WNvLjAwBggrBgEFBQcCARYkaHR0cHM6
Ly93d3cudWFuYXRhY2EuY29tL3B1YmxpYy9jcHMvMAgGBgQAj3oBAjCBjwYDVR0fBIGHMIGEMECg
PqA8hjpodHRwOi8vY3JsMS51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvQ0Eyc3Vib3JkaW5h
ZGEuY3JsMECgPqA8hjpodHRwOi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvQ0Ey
c3Vib3JkaW5hZGEuY3JsMA4GA1UdDwEB/wQEAwIHgDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAe
BgNVHREEFzAVgRN0c3BAdmFsaWRhdGVkaWQubmV0MA0GCSqGSIb3DQEBCwUAA4ICAQAbb2/wyumX
thPbzxQydCkWemTRAjKpW/fQFXBkY4+WnQzx7oEGgdO0HBzNc52AkxH36OvmKHEY2XbzQPYNbAHLK
gf0rq+tkB/3KBWqiqmxugL7mt00wMUqeIY+JS7IbTTwpx618qy7ynt7kqgUhkNGVlqJaYtvv
VmBMAZEu7WXjsm9gslyfsrt6F1FW/oOrnb8FA7MZN9FMcHzmfgjf0apBWJCVrAPzACMmAQkC3531h
jr6z1/VBDqye9/NomPqd6UZurGbmwwC9keGB7FMr+51snb0gSyWvy9GC0nYu4LW7dcmK1tFaRtt1d
hY546K1gJi7GO3xsBw1UXN6LQV6RNXStR9KF8YK5FazmFsMJ22bWl8IOyWyXC3bjRF6BN+US2N
iwIU2lD6Cbb3kT7U+B5ND/utHLcCA20PbjPTAGKRj7UR+jKdoSel/me0cV2WP3XWQRM/KQKgSJ
utnAM9vd1mZTuyFPv9ts51ypt5rto2L9EMXWBQ1YrefpXW6ZU4qJp7pNQsVV6LSV5FpbINCqu
Ba9Ih9z4urGVsJoD+4HFVN0ndWA4e2KId2CgmD2cwBVQon8gkmbFJZT1b/vIPUPiYy8dIIh3UpmEj
S9OsGhSIvJu25lAgJ2xEC5yMKY6kwPXfsDN/6cUR6RG+8lPYcz6v+j6ZQICcn6+Zww==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA2 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B65750721*

Subject CN: *VALIDATED ID QUALIFIED TSU01*

Subject OU: *VALIDATED ID TSP*

Subject O: *VALIDATED ID SL*

Subject L: *BARCELONA*

Subject C: *ES*

Valid from: *Tue Nov 26 18:45:11 CET 2019*

Valid to: *Fri Nov 26 18:45:11 CET 2027*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CA:F1:D8:EA:3C:95:70:23:8D:8D:19:AE:2F:1D:2A:E9:35:E4:46:AD:AD:A4:62:5E:3B:2E:D6:F4:05:6B:74:23:06:87:D1:13:0A:B3:D4:C9:05:30:96:27:D5:81:75:9E:04:E7:60:D2:F9:22:DA:BF:B1:D3:5D:B4:32:6D:6D:1E:2B:84:AE:6B:49:6D:CD:29:43:2A:D6:B7:BA:B6:AC:46:FF:91:6D:03:AB:14:EF:FC:C1:E0:99:3D:1A:26:27:B9:A0:2F:7D:3E:2B:15:5B:19:03:F1:D5:B3:9C:42:26:64:27:71:25:12:02:ED:DF:B5:34:7A:CF:00:45:5E:95:2B:AD:E3:15:68:A3:B5:F5:C4:48:EF:99:A0:78:2B:26:B4:E8:9F:AF:A7:BC:89:47:58:38:5F:E3:55:C4:00:9E:23:C2:DC:89:1C:69:A3:D4:C0:16:2A:B2:EF:A5:E7:BE:AF:94:46:95:34:76:5E:7A:8E:D3:29:BD:43:6C:34:CC:36:F3:A8:AB:F9:ED:95:C0:02:54:BB:FA:A4:C3:56:A3:21:CF:F0:A7:DF:F8:BD:FC:7A:A7:77:CD:05:31:70:C1:5D:CF:5F:7D:EB:DC:52:53:15:84:B2:AB:8B:17:E4:2C:FD:99:01:49:CD:9D:30:DE:85:F6:F9:12:1D:72:D9:4B:1B:02:03:01:00:01*

Authority Info Access

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *E8:51:4E:DD:BC:CC:78:9C:11:37:26:F3:CA:D8:98:E1:B8:58:9E:97*

Basic Constraints *IsCA: false*

Authority Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Certificate Policies

Policy OID: 1.3.6.1.4.1.47286.2.5

CPS text: [Certificado de sello de tiempo electrónico.]

CPS pointer: https://www.uanataca.com/public/cps/

Policy OID: 0.4.0.2042.1.2

CRL Distribution Points

http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl

http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *tsp@validatedid.net*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E3:00:17:A1:84:38:64:F7:C5:AE:60:4C:E2:12:61:39:C2:11:B4:D2:FE:F8:3E:F1:3E:DE:8F:72:57:B6:57:B3*

X509SubjectName

Subject 2.5.4.97: *VATES-B65750721*

Subject CN: *VALIDATED ID QUALIFIED TSU01*

Subject OU: *VALIDATED ID TSP*

Subject O: *VALIDATED ID SL*

Subject L: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *6FFO3bzMeJwRNybzytiY4bhYnpc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2020-04-28T00:00:00Z

38 - TSP: Entrust Datacard Europe S.L.U.

.

TSP Name

Name	[es]	*Entrust Datacard Europe S.L.U.*
Name	[en]	*Entrust Datacard Europe S.L.U.*

TSP Trade Name

Name	[en]	*VATES-B81188047*
Name	[en]	*Entrust Datacard Europe S.L.*
Name	[es]	*Entrust Datacard Europe S.L.*
Name	[en]	*Entrust Datacard Europe, S.L.*

PostalAddress

Street Address	[en]	*P.E. La Finca. Paseo del Club Deportivo, 1 Bloque 3 BJ*
Locality	[en]	*Pozuelo de Alarcón*
State Or Province	[en]	*Madrid*
Postal Code	[en]	*28233*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*P.E. La Finca. Paseo del Club Deportivo, 1 Bloque 3 BJ*
Locality	[es]	*Pozuelo de Alarcón*
State Or Province	[es]	*Madrid*
Postal Code	[es]	*28233*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*https://eu.entrustdatacard.com*
URI	[es]	*https://eu.entrustdatacard.com/es*
URI	[en]	*mailto:ecs.support@entrust.com*

URI	*[es]*	*mailto:ecs.support@entrust.com*

TSP Information URI

URI	*[en]*	*https://eu.entrustdatacard.com/resources/*

38.1 - Service (granted): Servicio de emisión de certificados autenticación de sitios web por "Entrust Certification Authority - QTSP1"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[es]*	*Servicio de emisión de certificados autenticación de sitios web por "Entrust Certification Authority - QTSP1"*
Name	*[en]*	*Service Website authentication certificate issued by "Entrust Certification Authority - QTSP1"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *207925336715604632050194166203739771814*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIE+DCCA+CgAwIBAgIRAJxs9pVwDGAAAAAAAFHTk6YwDQYJKoZIhvcNAQELBQAwgb4xCzAJBgNV
BAYTAlVTMRYwFAYDVQQKEw1FbnRydXN0LCBJbmMuMSgwJgYDVQQLEx9TZWUgd3d3LmVudHJ1c3Qu
bmV0L2xlZ2FsLXRlcm1zMTkwNwYDVQQLEzAoYykgMjAwOSBFbnRydXN0LCBJbmMuIC0gZm9yIGF1
dGhvcml6ZWQgdXNlIG9ubHkxMjAwBgNVBAMTKUVudHJ1c3QgUm9vdCBDZXJ0aWZpY2F0aW9uIEF1
dGhvcmlteSAtIFcyMB4XDTE5MDcyNjE4MzE0NVoXDTMwMTEyNjE5MDE0NVowgwYAxMDAuBgNVBAMM
J0VudHJ1c3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBRVFNQMTEYMBYGA1UEYQwPVkFURVMt
QjgxMTg4MDQ3MSUwIwYDVQQKDBxFbnRydXN0IERhdGFjYXJkIEV1cm9wZSBTLkwuMQswCQYDVQQG
EwJFUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANzuQL7uN0KUXjcflOAhX+kmgFVc
PzBSqzmrJpS23IM1KJCgVTQs8QyDvdMrfqAgAqvUhy6Q45JhRISFu8YUyucXfMXoab9f2LKHLlC
hYEy4Ixgei1I6VCpMv12udvpEDPtx3eLQJrWrnWVLtl40sGcBTml37AmTw+z3oiudEUlAL0Sb7L
IcQv3YPppb74mox2rFfzGhz+mzAKxE9dWznp/L8QeX1bQtbid5oImDwhFlnvS5KAvrxyEX5lWl8x
57BT4ISYbV5iP1/FY9y7Y0BemUxZ5niTJhi6QvcJx9uNBnca7j4WQsAmaVBDO1hFe7g9KJWZ94p
5dvW+iOytKUCAwEAAaOCASswggEnMA4GA1UdDwEBwQEAwIBhjASBgNVHRMBAf8ECDAGAQH/AgEA
MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjA7BgNVHSAENDAyMDAGBFUdIAAwKDAmBggr
BgEFBQcCARYaaHR0cDovL3d3dy5lbnRydXN0Lm5ldC9ycGEwMwYIKwYBBQUHAQEEJzAlMCMGCCsG
AQUFBzABhhdodHRwOi8vb2Nzcc5lbnRydXN0Lm5ldDAwBgNVHR8EKTAnMCWgI6Ahhh9odHRwOi8v
Y3JsLmVudHJ1c3Qubm V0L2cyY2EuY3JsMB0GA1UdDgQWBBQcrT+c1y0iGaGcS+na8Soz9/u6DTAf
BgNVHSMEGDAWgBRqcIZ6IB7vfec7aVHUbI2kBJmqzANBgkqhkiG9w0BAQsFAAOCAQEAJhhuoOOr
p7VZX+7gzDsbRLV7sbkiDZTktBg23+trxG/lj93NsjQkpRRoUCH5HsmeaqhztZWAv47ez53VrT/H
zqECST4Yae2HDFysNaXGkBnV2HbCbjWEDxMB9HWIR1FM0K0l1wtY724NU+BqsDQL92JXxRllGYQF
vUjSyddL/EcKFyNWiah7BakLELC/P/V8C927byrCARGEOkeMYoA6YnMDWpQX12eRJCMuXzrSRzl7T
HoRprTZGX2RaPJpqjnCfEzU/8xJcFaaCBXruhdfAv5ew6aEcJ0IiFkEgGW1xPljibwn6A/BaOe0
xsAudqAjLTQh/9xQnaAdrK6bxqxGRQ==

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Entrust Root Certification Authority - G2*
Issuer OU:	*(c) 2009 Entrust, Inc. - for authorized use only*
Issuer OU:	*See www.entrust.net/legal-terms*
Issuer O:	*Entrust, Inc.*
Issuer C:	*US*

Subject C:	*ES*
Subject O:	*Entrust Datacard Europe S.L.*
Subject 2.5.4.97:	*VATES-B81188047*
Subject CN:	*Entrust Certification Authority - QTSP1*
Valid from:	*Fri Jul 26 20:31:45 CEST 2019*
Valid to:	*Tue Nov 26 20:01:45 CET 2030*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DC:EE:40:BE:EE:37:42:94:5E:37:1F:20:E0:21:5F:E9:26:80:55:5C:3E:00:52:8E:AC:E6:AC:4A:79:DB:72:0C:D4:A2:02:81:54:D0:B0:94:32:0E:F7:4C:B7:4A:80:80:0A:AF:52:1C:BA:43:8E:49:85:12:12:16:EF:18:53:2B:9E:5D:F3:17:A1:A6:DF:F7:62:CA:1C:B7:C2:85:81:32:E0:8C:60:7A:2D:48:E9:50:A9:32:FD:76:B9:DB:E9:10:33:ED:C7:77:8B:40:9A:D6:AE:75:95:2E:D9:78:D2:C1:9C:05:39:88:DF:B0:26:4F:0F:B3:DE:88:AE:74:45:08:00:B2:34:49:B4:CB:21:C4:2F:DD:83:E9:A5:BE:F8:9A:8C:76:AC:57:F3:1A:1C:FE:9B:30:0A:C4:4F:5D:5B:39:E9:FC:BF:10:79:7D:5B:42:D6:E2:77:9A:08:98:3C:21:16:59:EF:4B:92:80:BE:BC:72:11:7E:65:5A:5F:31:E7:B0:53:E1:F4:98:85:5E:62:3F:5F:C5:63:DC:BB:63:40:5E:99:4F:F1:67:99:E2:4C:98:62:6D:0B:DE:27:1F:6E:34:19:DE:6B:B8:F8:59:0B:00:99:A5:41:0C:ED:61:15:EE:E0:F4:A2:56:67:DE:29:E5:DB:D6:FA:23:B2:B4:A5:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Extended Key Usage	*id_kp_serverAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.entrust.net/rpa*
Authority Info Access	*http://ocsp.entrust.net*
CRL Distribution Points	*http://crl.entrust.net/g2ca.crl*
Subject Key Identifier	*1C:AD:3F:9C:D7:2D:22:19:A1:9C:4B:E9:DA:F1:2A:33:F7:FB:BA:0D*
Authority Key Identifier	*6A:72:26:7A:D0:1E:EF:7D:E7:3B:69:51:D4:6C:8D:9F:90:12:66:AB*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*68:1E:BC:18:22:B0:79:B9:7E:04:04:E4:68:7D:9B:6C:0C:08:92:C8:20:F5:57:38:A2:82:AA:E6:25:29:BD:D8*

X509SubjectName

Subject C:	*ES*
Subject O:	*Entrust Datacard Europe S.L.*
Subject 2.5.4.97:	*VATES-B81188047*
Subject CN:	*Entrust Certification Authority - QTSP1*

X509SKI

X509 SK I	*HK0/nNctIhmhnEvp2vEqM/f7ug0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time *2020-07-28T00:00:00Z*

38.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

38.2 - Service (granted): Qualified Certificates issued by "Entrust Certification Authority - ES QSig1"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by "Entrust Certification Authority - ES QSig1"*

Name *[es]* *Certificados cualificados emitidos por "Entrust Certification Authority - ES QSig1"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *91144490788361283369824551057333035359*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGozCCBlugAwIBAgIQRJHKWCW+eYQrKbDDcoYhXzANBgkqhkiG9w0BAQ0FADBXMTAwLgYDVQQD
DCdFbnRydXN0IENlcnRpZmlj YXRpb24gQXV0aG9yaXR5IC0gQUFUTDExFjAUBgNVBAoMDUVudHJ1
c3QsIEluYy4xCzAJBgNVBAYTAlVTMB4XDTIwMDcyOTE2MzMwMFoXDTM3MTIzNTkwMFowgYQx
MzAxBgNVBAMTKkVudHJ1c3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBFUyBRU2lnMTEYMBYG
A1UEYRMPVkFURVMtQjgxMTg4MDQ3MSYwJAYDVQQKEx1FbnRydXN0IERhdGFjYXJkIEV1cm9wZSwg
Uy5MLjELMAkGA1UEBhMCRVMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC0G/GJ++yx
CAnevmBeXkBPJL7v+cgA+DUFjNLKkkfGuYQkrSSQVcfx5+TEoOYN+Hy7Sz/y6FG6gy0kcJ0n094
/FPyTJHS8D5sD38LDgRgkUzplEpt3zYTCBCgbDZDpb0TqPIX+6RLO+Jo/BtyFMKVwVEIMwmZx0sK
CPl4mPyTLUIpGuU9OV1irqMOCOtVl4117FuySw3vaeDtX+rQKCPQx2J5Wzg4mSUXGbAr86dMncjx
pwm5A29Tmff3VUEzmAeQAOX/Q+qQmnAI2Dp9Nj/pk78RmwXLmq09l+jIfzRJbC7ov2EtUMmJApPU
DQT2Vs8zc/JG92UHQlTbdSebIAT+At2dmVaykMWfiZ8s7TauoeEnDPNr321uddC1zS+SxKANLdg2
2Pz3I4Ke6zqq5IYBy8Iswz4p6cCBRFotjpr9wDSVFj4pTeKJsf6LDb8kUExwvtxXCUXUqJenCXn7VP
2qNwxcERX0OaCjzivpu1+x68vFiajkV5QQyAHowZatPJ4iDPar4a9bFLLo0sLrlCs0ukDRyS1cnj
bE8nB/mQVC97SqP/VtzceatzOxJFlxpViSqXrq005zMkbKUFgZ9lcU8UMcvJyMt34NSi25xmgOo
MUMLVVzlkxb5IY+bPks6OYar7WoHh8TKB0VkNHQOc2jHdzldRsRNd2sZLFtL9XtWwIDAQABo4IB
OzCCATcwDgYDVR0PAQH/BAQDAgEGMCoGA1UdJQQjMCEGCCsGAQUFBwMEBgorBgEEAYI3CgMMBgkq
hkiG9y8BAQUwEgYDVR0TAQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUWlMImEwqQ3q1UOX05g7lR4u
bQIwHwYDVR0jBBgwFoAUY/GE3QO+o59k+nZ6R8RWlsBtoCAwMwYIKwYBBQUHAQEEJzAlMCMGCCsG
AQUFBzABhhodHRwOi8vb2NzcC5lbnRydXN0Lm5ldDAzBgNVHR8ELDAqMCegJqAkhiJodHRwOi8v
Y3JsLmVudHJ1c3QubmV0L2FhdGwxY2EuY3JsMDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYGCCsGAQUF
BwIBFhpodHRwOi8vd3d3LmVudHJ1c3QubmV0L3JwYTANBgkqhkiG9w0BAQ0FAAOCAgEAaPxyjsae
gc83/3wCW7HMXmPSMPdB6bEYO5kOdPLbdbaBNJM2LuGSbv+Doxqbulsnk/jS1+rVpTn/xAawEotf
E0pF2U1iLpzPgrH5Mew/f1yf8+JoPP98wuWQ3eHyVCSNpTdyE5tr7s2QNV6o6Yrie7HlI/l9vE6qZ
vzlkXh3iN/oOWo/zWbo5NImZOIDy/nNCIh+xT4VXcEI9SDdo0ucoCLKe7exfGz5tacgvEOtsn+wRD
kXP8G5cxwbWWh9VsoRUsmDahckJsFxJ0Cqno8Qt1muk/a7MMWwDf0OAQPyW7+jdW3Wma7qJnG3v
7mDetHxQ7B3lMUAurDJsIZNcJ8KUl0wWlBpriGXoLsb8fVlQvbxcsfxTreCXf6Xqrt6/aogMwiqT
g4FnlL5iboRU0r2h1Zei9ePSsaspCTgHnSlzBNVx6+SYNSlHPkEg3FPmIPbKLYkeTJb4lÛ9F+d
LINPKtLnHvVFMbecS7qs1M8l9ltSXsrK rt4rqUiQ1SEBQrwitaXDzYkGGw/4v+ezab9HVb0VQ7X8
9iyY+KJVRPFJ9aDtmaHSzMQiduSAy7bGBT6LFN8dUE3qqDVdZFwU5VW6L9y76lhoile/tOVH+gLB
fh5SqKmmIUvd6eYlGG59743qOeiP8Yct67apk9HadUSQ8STL7Vj3zzD2yZfrh00jmA=

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer C: *US*

Issuer O: *Entrust, Inc.*

Issuer CN: *Entrust Certification Authority - AATL1*

Subject C: *ES*

Subject O: *Entrust Datacard Europe, S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - ES QSig1*

Valid from: *Wed Jul 29 18:33:00 CEST 2020*

Valid to: *Sun Dec 20 00:59:00 CET 2037*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B4:1B:F1:89:FB:EC:B1:08:09:DE:BE:60:5E:5C:A9:4F:24:BE:F2:F9:C8:00:F8:35:05:8C:D2:CA:92:47:C6:B9:84:24:AF:94:90:55:C2:31:E7:E4:C4:A0:E6:0D:F8:7C:BB:4B:3F:F2:E8:51:BA:83:2D:24:78:98:F4:9F:4F:78:FC:53:F2:4C:91:D2:F0:3E:6C:0F:7F:0B:0E:04:60:91:4C:E9:94:4A:6D:DF:36:13:08:10:A0:6C:36:43:A5:BD:13:A8:F2:17:FB:A4:4B:3B:E2:68:FC:1B:72:14:C2:95:C1:51:25:33:09:99:C7:4B:0A:08:F9:78:98:FC:93:2D:42:29:1A:E5:3D:39:5D:62:AE:A3:0E:08:EB:55:23:8D:5F:EC:5B:B2:4B:0D:EF:69:E0:ED:5F:EA:D0:28:23:D0:C7:62:79:5B:38:38:99:25:17:19:B0:2B:F3:A7:4C:9D:C8:F1:A7:09:B9:03:6F:53:99:F1:77:55:41:33:98:07:90:00:E5:FF:43:EA:90:9A:70:08:D8:3A:7D:36:3F:E9:93:BF:11:9B:05:CB:9A:AD:3D:97:E8:E5:7F:34:49:6C:2E:E8:BF:61:2D:50:C9:89:02:93:D4:0D:04:F6:56:FF:33:73:F2:46:F7:65:07:42:54:DB:77:97:A1:20:04:FE:02:DD:9D:99:56:B2:90:C5:9F:89:9F:2C:ED:36:AE:A1:E1:29:0C:F3:6B:DF:6D:6E:75:D0:B5:CD:2F:92:C4:A0:0D:2D:DA:B6:D8:FC:F7:23:82:BA:CE:9A:B9:21:80:63:F0:8B:30:CF:8A:7A:70:20:51:16:87:E9:AF:DC:03:49:51:63:E2:94:DE:2A:5B:08:E8:B0:E1:48:A5:04:C7:0B:ED:BD:70:94:5D:4A:89:7A:70:97:9F:B5:4F:DA:A3:70:C5:E1:11:5F:43:9A:0A:3C:E2:BE:9B:B5:FB:1E:BC:BC:57:DA:8E:45:79:41:0C:80:1E:8C:19:6A:D3:C9:E2:20:CF:6A:BE:1A:F5:B1:4B:2E:8D:2C:2E:B9:42:B3:4B:A4:0D:1C:92:D5:C9:E3:6C:4F:27:07:FA:E7:41:50:BD:EF:9A:8F:FD:5B:73:71:E6:AD:CC:EC:49:16:5C:69:56:24:AA:5E:BA:B4:D3:9C:CC:91:B2:94:16:06:7D:95:C5:3C:50:C7:2F:27:23:2D:DF:83:52:8B:6E:71:9A:03:A8:31:43:0B:55:5C:FF:93:16:F9:21:8F:A1:3E:4B:3A:39:86:AB:ED:6A:07:87:C4:CA:07:45:64:34:74:0E:73:68:C7:E3:37:DD:46:C4:4D:77:6B:09:D8:B1:6D:2F:D5:ED:5B:02:03:01:00:01

Extended Key Usage *id_kp_emailProtection - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *5A:53:08:8A:61:30:A9:0D:EA:D5:43:97:D3:98:3B:95:1E:2E:6D:02*

Authority Key Identifier *63:F1:84:DD:03:BE:A3:9F:64:FA:76:7A:47:C4:56:7E:C0:6D:A0:20*

Authority Info Access *http://ocsp.entrust.net*

CRL Distribution Points *http://crl.entrust.net/aatl1ca.crl*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://www.entrust.net/rpa

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B2:87:4B:58:8A:94:03:47:98:31:9D:5D:32:9D:B2:65:F8:3A:47:F3:15:BA:58:31:A4:97:0C:B5:71:66:D5:94*

X509SubjectName

Subject C: *ES*

Subject O: *Entrust Datacard Europe, S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - ES QSig1*

X509SKI

X509 SK I *WlMIimEwqQ3q1UOX05g7lR4ubQI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-07-01T01:00:00Z

38.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

38.3 - Service (granted): Qualified Certificates issued by "Entrust Certification Authority - ES QSeal1"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by "Entrust Certification Authority - ES QSeal1"*

Name *[es]* *Certificados cualificados emitidos por "Entrust Certification Authority - ES QSeal1"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *264921645305930525180157359667800362 67*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGpDCCBIygAwIBAgIQE+40jkkvyda1xJzwc/cUqzANBgkqhkiG9w0BAQ0FADBXMTAwLgYDVQQD
DCdFbnRydXN0IENlcnRpZmlyYXRpb24gQXV0aG9yaXR5IC0gQUFUTDExFjAUBgNVBAoMDUVudHJl
c3QuIEluYy4xCzAJBgNVBAYTAlVTMB4XDTIwMDcyNzE0MzkwN1oXDTM3MTIxOTIzNTkwMFowgYUx
NDAyBgNVBAMTK0VudHJlc3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBFUyBRU2VhbDExGDAW
BgNVBGETD1ZBVEVTLUI4MTE4ODA0NzEmMCQGA1UEChMdRW50cnVzdCBEYXRhY2FyZCBFdXJvcGUs
IFMuTC4xCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2dFdf4p
YIZXbIeFzTcnigA/dvDzFrIkMwS1WSAUJRCGUt6MVF9ZBN9T61qyp/qKImn8I2ePPOJaFFrkAdi
Xg71cI/pxiA8rMh9ioUZFdqtPTQlwfmYJUZRooiNbQVEKbqkr+ETXuYYH8jtI81mRkxsRkeH7PL
cglEcwGsDxr4k5fdneMG9lIJdmbGt3llzeb7ThwrM0rcvX/qZnuL26+6dRrfGPqmUcFpp3w0jMXg
x4MILMMblqgW47zAsl4dVbvIHYlrUecZJ13kGm/dFRVqf7knmJYz+O+oBYbQqfCif8kFg3DeUlhyX
OdqVU9vTNfOE6OyysCrhs1LfAXaEDSUhxoKKidAiwgurDIBEMkKUX7an8u+x7nB4s7K24rcJwls
rA51i7SK/O4kHOnK3JTjTSGbgrwahEco/Ndtn6M1y9AHSpaNZq5I3hkgBJoK3Ya1DILUnMSNO+ag
GnzJR1HWQEWfLT19eiEh70vo96y5KLOPhsBlpV6txLehL8DaQvF6HK+RD7ev+TZo3VXrwpXiS2Hv
HZR2LmIudY9uVxY4HHD0KXWIKJzpN4Oq9vBmXYpCdbHqWA8pUi60sMc2+Snc9qO2uTsLBSnT161eqw
XUK+hnHj3RqtsL14vIT28Teseq2OUETDLOiUO7KgFgsBrIcpA0rwuEljc4ysWE/j8sCAwEAAaOC
A1swggE5MA4GA1UdDwEB/wQEAwIBhjAqBgNVHSUEIzAhBggrBgEFBQcDBAYKKwYBBAGCNwoDDAYJ
KoZIhvcvAQEFMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFFaAFSOVcX/nLZDQzQY6T2dj
fT11MB8GA1UdIwQYMBaAFGPxhN0DvqOtZPp2ekfEVn7AbaAgMDMGCCsGAQUFBwEBBCcwJTAjBggr
BgEFBQcwAYYXaHR0cDovL29jc3AuZW50cnVzdC5uZXQwMwYDVR0fBCwwKjAooCagJIYiaHR0cDov
L2NybC5lbnRydXN0LmS1dC9hYXRsMWNhLmNybDA7BgNVHSAENDAyMDAGBFUdIAAwKDAmBggrBgEF
BQcCARYaaHR0cDovL3d3dy5lbnRydXN0LmS1dC9ycGEwDQYJKoZIhvcNAQENBQADggIBAEa5I5j6
+v8us3u+jNXuF+URtl+RLUD4jFIf4fRnyUqGeIUjfQFLyJe/NUBOOm+LZQx5/pr/p+Bo2O5HPUcl
dQLLWoOd8AZIbO1XYnIGLNMHiJwEmKLkxiLvCAlgvVerymDIRXQTh0L/vu8g+R73Mlx+714RioW8U
Hzs2H9bXuqVDYgBf686dXI/c9MGEsfCvOh6+LaqtCziECdxQbfzEOmI+SLSxNAoKcGRhk75XHoI
ZdtWYT4nbP74P/i6nQdRW7iPJE1ZFx00dEhb070F3s4Nx+X+bbSWIARoNiZqPZUghBWYw3j8l78
66ULNHjd9N0VccjqWQhK0/e4sHnbDcLYAIqJ/ox+vT1lsxXxaX1VN+v2NK8auqsuLZeE+sIRAg8Y
0S7HPCcRbFqM14sGR8SL6fImuITtbSW34jtP1goRE2hFHTBgys29JvWislnqaNvt1h7zWZp/Rj/
E9uxgdcQ0IMTQbAv0A/IbVtJIn1ATxH74qHEAgMagbmFqOLe2rrIeu03dLuHXLjgen22G4ySg8Ya
z4NQmdymcO64eVPcXThKjMUHHwrf+IZNmhboGQK7W7D+qMUd1nyOGLfq347c6kbPmRLfO6btRNaW
tROtzDoWFX6WWvCIZfLEXiepal8yjaO3yN6rEk96pgOZU7litxSm0o2L4BryuD4fqORf
-----END CERTIFICATE-----
```

Signature algorithm:	*SHA512withRSA*
Issuer C:	*US*
Issuer O:	*Entrust, Inc.*
Issuer CN:	*Entrust Certification Authority - AATL1*
Subject C:	*ES*
Subject O:	*Entrust Datacard Europe, S.L.*
Subject 2.5.4.97:	*VATES-B81188047*
Subject CN:	*Entrust Certification Authority - ES QSeal1*
Valid from:	*Mon Jul 27 16:39:07 CEST 2020*
Valid to:	*Sun Dec 20 00:59:00 CET 2037*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D9:D1:5D:7D:FE:29:62:56:57:7D:BB:5E:17:34:DC:9E:28:00:FD:DB:C3:A0:5A:DF:90:CC:39:21:64:80:51:47:D1:08:65:3A:31:51:7D:64:13:7D:4F:AD:6A:CA:9F:EA:28:89:E6:F1:FD:9E:3C:F3:88:68:51:6B:90:07:62:5E:0E:F5:78:9F:E9:C6:20:01:AC:C8:7D:8A:85:19:15:DA:AD:3D:34:25:C1:F9:98:25:46:51:A2:88:8D:6D:05:44:2A:1A:A4:8B:E1:13:5E:E6:18:1F:C8:ED:23:CD:66:46:4C:6C:46:47:87:7F:B3:CB:72:09:44:73:01:AC:0F:1A:F8:93:97:DD:9D:E3:06:F6:52:09:76:66:C6:B7:79:48:CD:E6:FB:4E:1C:2B:33:4A:DC:BD:7F:EA:66:7B:8B:DB:AF:BA:75:1A:DF:18:FA:A6:51:C1:69:A7:7C:34:8C:C5:E0:C7:83:25:2C:C3:1B:96:AA:96:E3:BC:C0:B2:5E:1D:55:BB:C8:1D:89:6B:51:E7:99:27:5D:E4:1A:6F:DD:15:15:6A:7F:B9:27:98:96:33:F8:EF:A8:05:86:D0:A9:F0:A2:7F:C9:05:83:70:DE:52:1C:97:39:DA:95:53:DB:D3:36:D3:84:E8:EC:B2:B0:2A:E1:B3:52:DF:01:76:84:0D:25:21:C6:82:8A:B5:D0:22:DF:08:2E:AC:32:01:10:C9:0A:51:7E:DA:9F:CB:BE:C7:B9:C1:E2:CE:CA:DB:8A:DC:27:09:6C:AC:0E:75:8B:B4:A4:FC:EE:24:7C:E9:C8:38:94:E3:4D:21:9B:82:BC:1A:84:47:28:FC:D7:6D:9F:A3:35:CB:D0:07:4A:96:8D:66:AE:65:DE:19:20:04:9A:0A:DD:8B:B5:0C:82:D4:9C:C4:8D:3B:E6:AA:1A:7C:C9:47:51:D6:40:45:9F:2D:3D:7D:7A:21:21:EF:4B:E8:F7:AC:B9:28:B3:8F:86:C0:65:A5:5E:AD:C4:B7:A1:2F:C0:DA:42:F1:7A:1C:AF:91:0F:B7:AF:F9:36:68:DD:55:EB:C2:95:E2:4B:61:EF:1D:94:76:2E:62:2E:75:8F:6E:57:16:38:1C:70:F4:29:75:88:28:9C:E9:37:83:AA:F6:F0:66:5D:8A:42:75:B1:EA:58:0F:29:53:AD:2C:31:CD:BE:4A:77:3D:A8:ED:AE:4E:C2:C1:4A:74:FA:D5:EA:B0:5D:42:BE:86:71:E3:DD:1A:AD:B0:BD:78:BE:54:F6:F1:37:AC:7A:AD:8E:50:44:C3:2F:48:94:3B:B2:A0:16:0B:01:7F:57:29:03:4A:F0:8A:E1:25:8D:CE:32:B1:61:3F:8F:CB:02:03:01:00:01*
Extended Key Usage	*id_kp_emailProtection - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*56:80:15:23:95:71:7F:E7:2D:90:D0:CD:06:3A:4F:67:63:7D:3D:75*
Authority Key Identifier	*63:F1:84:DD:03:BE:A3:9F:64:FA:76:7A:47:C4:56:7E:C0:6D:A0:20*
Authority Info Access	*http://ocsp.entrust.net*
CRL Distribution Points	*http://crl.entrust.net/aatl1ca.crl*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.entrust.net/rpa*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*17:01:DE:38:12:4C:44:58:F3:2B:88:AE:7E:62:AC:15:87:6C:42:7A:3A:D3:BB:AE:8F:D1:47:9F:F0:00:30:F3*

X509SubjectName

Subject C:	*ES*
Subject O:	*Entrust Datacard Europe, S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - ES QSeal1*

X509SKI

X509 SK I *VoAVI5Vxf+ctkNDNBjpPZ2N9PXU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-07-01T01:00:00Z

38.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

39 - TSP: EVICERTIA S.L.

.

TSP Name

Name	*[en]*	*EVICERTIA S.L.*
Name	*[es]*	*EVIDENCIAS CERTIFICADAS S.L.*

TSP Trade Name

Name	*[en]*	*Evicertia*
Name	*[es]*	*Evicertia*
Name	*[en]*	*VATES-B86021839*
Name	*[es]*	*VATES-B86021839*
Name	*[en]*	*EVIDENCIAS CERTIFICADAS S.L.*

PostalAddress

Street Address	*[es]*	*C/Lagasca, 95*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28006*
Country Name	*[es]*	*ES*

PostalAddress

Street Address	*[en]*	*C/Lagasca, 95*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28006*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:info@evicertia.com*
URI	*[es]*	*mailto:info@evicertia.com*

URI	*[en]*	*http://www.evicertia.com*
URI	*[es]*	*http://www.evicertia.com*

TSP Information URI

URI	*[en]*	*http://www.evicertia.com*
URI	*[es]*	*http://www.evicertia.com*

39.1 - Service (granted): Qualified timestamps issued by EVITSU-QE1A

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified timestamps issued by EVITSU-QE1A*
Name	*[es]*	*Sellos de tiempo cualificados emitidos por EVITSU-QE1A*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*6314744856537535544*
X509 Certificate	


```
-----BEGIN CERTIFICATE-----
MIIHHTCCBQWgAwIBAgIIV6J6/XUlFDgwDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJlyZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5B1jEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQU5BVEFDQSBDQTIgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzfxNDk5MB4X
DTE5MTEyMDEwMjgzNVoXDTI5MTEyMDEwMjgzNVowgaExCzAJBgNVBAYTAkVTMQ8wDQYDVQQHDAZN
QURSSUQxJTAjBgNVBAoMHEVWSURFTkNJQVMgQ0VSVEIGSUNBREFTIFMuTC4xKjAoBgNVBAsMIUVW
SUNFUlRJQSBDTE9VRCBRVUFMSUZJRUQgVFNBIFFFMTEUMBIGA1UEAwwLRVZJVFNVLVFFMUExGDAW
BgNVBGEMD1ZBVEVTLU14NjAyMTgzOTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAO1G
1VPomFFNIS+GEGbzMXSDiR+n1Ifio/f+Gbz7t/lk40SS9eMNYt3+OznGsMBioIwuZipTwf0bt9mRF
4vCgJXWT3HgfOF+9Qjv7finnYioTkiQqimGHUQlcDgtfOXCarBZMUpxXBePpPc4KK7YaqwZkJgnEw
8RtEXnPlrtPqq65MK4BkGsYxsm3Ri73NK13hJbB6cRWczSN1yM7MqQ/BQcB98sBCayUL6Mjch7Ds
dQkRiUqM7jCgwFWdyvZsN5LGpwWWZU0FCZlB2bwo3Zddp+RkdMQ0tuYV6iFB7L0+TvFdLT9jEqb
vfUFM3+MPLTqQuOntHB7X6ZNob574pfrkCAwEAAaOCAj4wggf6MH4GCCsGAQUFBwEBBHIwcDA2
BggrBgEFBQcwAYYqaHR0cDovL29jc3AxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AvMDYG
CCsGAQUFBzABhipodHRwOi8vb2NzcDludWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wHQYD
VR0OBBYEFEQs4ki5yy5isrWSKEefNMqmKdNHMA4GA1UdEwQCMAAwHwYDVR0jBBgwFoAUiVfnYHPO
B0ap4qNo8OERsnSSc/0wgZMGA1UdIASBizCBiDBSBgorBgEEAYLxNgIFMG4wOgYIKwYBBQUHAgIw
LgwsQ2VydGlmaWNhZG8gZGUgc2VsbG8gZGUgdGllbXBvIGVsZWN0csOzbmljby4wMAYIKwYBBQUH
AgEWJGh0dHBzOi8vd3d3LnVhbmF0YWNhLmNvbS9wdWJsaWMvY3BzLzAIBgYEAI96AQIwgY8GA1Ud
HwSBhzCBhDBAoD6gPIY6aHR0cDovL2NybDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvY3JsL0NB
MtNJYm9yZGluYWRhLmNvbDBAoD6gPIY6aHR0cDovL2NybDIudWFuYXRhY2EuY29tL3B1YmxpYy9w
a2kvY3JsL0NBMtNJYm9yZGluYWRhLmNvbDAOBgNVHQ8BAf8EBAMCB4AwFzYDVR0JAQH/BAwwCgYI
KwYBBQUHAwgwHQYDVR0RBBYwFIESaW5mb0BldmljZXJ0aWEuY29tMA0GCSqGSIb3DQEBCwUAA4IC
AQCKTbKqj/vDUcOn0h/wbTqdHhyh7z9haRGMVuDZp2gGo5JtHC5QVFcMc6cdZTurRUzOmuluF4Y
uygy4EB03bVTLEWbSazDBcOjsfkS0+009b9cYLLltNdr/Fx+VHmRzsxOmmMldfh54fUlIY61dsFNR
uDKoFgwJCMPPwcsaPw7ZJBC2nqyFqcPHhr39QKgMEHsOJeS4PDp+JZGTs6fXodGHEQ46bYhMVjz
AO+lxNjZfEpJENXiCE466KmxdaTXAupBRwvYv+eCKGkGBgtV3rbHyAaDFAzOWfAGp5mjT3quQTbG
uuw+jvAvVT1zmRQlFSbNcOT6YNFWQLyu6cgq8CrGD/91g8a3wTvJVc2q9hxvredDLdDQwTeh3XP1
LqOCV9xtUhUVMJXvPWNljZIq21y/54Bi5UPEhrpvFM0JT1rzsPAjcPbvo0UM2Yr2lhmaIwmmky8
bQRCa0CDmUPDFvieCC1nYvIYgILZ3b8mWUmk8Tm/Du1B0AsYFqbc5OGwZIwtOMacYi9Ibsv8W3
lZtiQiENce2JmphakWiu9PRQb7NN5kP4UU3EJZuF7QAa8NFm5PYhq5Uppamtu2fzaroivi7lG5
4bWKw5UpZL2v9RN8fzYQyMTBPGqqNv4Cd4c87+5mfhpHZ3n0611xTqOg9lqDgls9tFzodJNITYv
ig==

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA256withRSA*
Issuer 2.5.4.97:	*VATES-A66721499*
Issuer CN:	*UANATACA CA2 2016*
Issuer OU:	*TSP-UANATACA*

Issuer O:	*UANATACA S.A.*
Issuer L:	*Barcelona (see current address at www.uanataca.com/address)*
Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-B86021839*
Subject CN:	*EVITSU-QE1A*
Subject OU:	*EVICERTIA CLOUD QUALIFIED TSA QE1*
Subject O:	*EVIDENCIAS CERTIFICADAS S.L.*
Subject L:	*MADRID*
Subject C:	*ES*
Valid from:	*Wed Nov 20 11:28:35 CET 2019*
Valid to:	*Sat Nov 20 11:28:35 CET 2027*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:ED:46:D5:53:E8:98:51:4D:21:2F:86:10:66:F3:31:74:83:7D:1F:A7:D4:87:E2:A1:77:FE:19:BC:FB:AD:49:38:7F:C4:BD:AC:C3:55:B7:7F:8E:CE:71:AC:30:18:A8:97:0B:B6:1A:94:F0:7C:E6:C8:F6:64:45:E2:F0:A0:25:75:93:DC:78:1F:38:5F:BD:42:3B:FB:7E:69:D8:8A:84:E4:89:0A:A2:8A:71:87:51:09:5E:0E:07:CE:5C:26:AB:05:93:14:A7:15:C1:78:FA:4F:73:82:8A:ED:86:AA:C1:99:09:82:71:30:F1:1B:44:5E:73:C8:AE:D3:EA:AB:AE:4C:2B:80:64:1A:C6:31:B2:6D:D1:8B:BD:CD:2B:5D:DB:25:B0:7A:71:15:9C:CD:23:75:C8:CE:CC:A9:0F:C1:41:C0:7D:F2:C0:42:6B:25:0B:E8:C8:DC:87:B0:EC:75:09:11:89:4A:8C:EE:30:A0:C0:55:9D:FF:2B:D9:B0:DE:4B:1A:9C:16:59:95:34:14:26:65:07:66:EF:A3:76:5D:76:9F:91:91:D3:10:D2:DB:98:57:A8:85:07:B2:F4:F9:3B:C5:74:B4:FD:8C:4A:9B:BD:F5:05:33:7F:8C:3C:B7:D3:A9:06:8E:9D:F1:C1:ED:7E:99:B4:DA:21:E7:BE:29:7E:B9:02:03:01:00:01*
Authority Info Access	*http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*44:2C:E2:48:B9:CB:2E:62:B2:B5:92:28:47:9F:34:CA:A6:29:D3:47*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.47286.2.5* *CPS text: [Certificado de sello de tiempo electrónico.]* *CPS pointer: https://www.uanataca.com/public/cps/* *Policy OID: 0.4.0.2042.1.2*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl* *http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*
Extended Key Usage	*id_kp_timeStamping*
Subject Alternative Name	*info@evicertia.com*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *35:2C:E0:7F:3D:6F:31:AC:2E:48:4F:82:66:BD:4A:6A:1E:ED:1F:B8:AC:E9:7D:39:19:DD:8C:D4:47:D6:D5:DF*

X509SubjectName

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVITSU-QE1A*

Subject OU: *EVICERTIA CLOUD QUALIFIED TSA QE1*

Subject O: *EVIDENCIAS CERTIFICADAS S.L.*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *RCziSLnLLmKytZIoR580yqYp00c=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-07-28T00:00:00Z

39.2 - Service (granted): Qualified timestamps issued by EVITSU-QE1B

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by EVITSU-QE1B*

Name *[es]* *Sellos de tiempo cualificados emitidos por EVITSU-QE1B*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7645472127858035635*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHHTCCBQWgAwIBAgIIahosZJEgy7MwDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmFpaKHNlZSBjdXJvZW50IGFkZHUlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEYMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQUSBVEFDQSBDQTIgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzIxNDk5MB4X
DTE5MTEyMDEwMjkyNFoXDT13MTEyMDEwMjkyNFowgaExCzAJBgNVBAYTAkVTMQ8wDQYDVQQHDAZN
QURSSUQxQTAjBgNVBAoMHEVMSUBFTkNJQVMgQ0VSVEIGSUNBREFTIFMuTC4xKjAoBgNVBAsMIUVW
SUNFUlRQSBDTE9VRCBRVUFMSUZRTQgVFNBIFFFMTEUMBIGA1UEAwwLRVZJVFNVLVFFMU1ltxGDAW
BgNVBGEMDlZBVEVTLUl4NjAyMTgzOTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPx
GUbAvwc3nJtvoPYPYFYq7MLjxRtNlp7iMzFL3lKTWeTrmpVMS9tbrCRmY2X3BPgjA0gSBPpoqDU
AB+xBtb+xqbCrkE4DQC8K48I20ts2NWALAIWaqemfiuJe3OXcctF0Iy6lANz1DV+EmLx7Iyz2e+P
AntkAnqNC1Ds8PlApMLDE6VvTMMBPwwIMjBLmngUxKaVS9np/5kq2mfcWcuR+YRETuqZTEo40
vZxhfkaJMFhj6mXg55QAxl0U5dCMg/PeBzIvdRPBKesi3z20q5irj+vxY0vRrRvOcT7SKssGfmM
L2aHKAWvg46GEhHELj5oBv7sI3S3X8bar0cCAwEAAaOCAj4wggI6MH4GCCsGAQUFBwEBBHIwcDA2
BggrBgEFBQcwAYYqaHR0cDovL29jc3AxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AvMDYG
CCsGAQUFBzAChipodHRtOi8vb2Nzc0luaWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2Nzc3wuHQYD
VR0OBBYEFCaVISQvipDibOP3a+dDo0c90CTaMAkGA1UdEwQCMAAwHwYDVR0jBBgwFoAUfVfnYHPO
B0ap4qNo8OERsnSSc/0wgZMGA1UdIASBizCBiDB8BgorBgEEAYLxNglFMG4wOgYIKwYBBQUHAgIw
LgwsQ2VydGlmaWNhZGSgZGUgc2VsbG8gZGUgdGlhXBv1GVsZWN0csOzbmljby4wMAYIKwYBBQUH
AgEWJGhtdHBzOi8vd3d3LnVhbmF0YWNhLmNvbS9wdWJsaWMvY3BzLzAIBgYEAI96AQIwgY8GA1Ud
HwSBhzCBhDBAoD6gPIY6aHR0cDovL2NybDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvY3JsL0NB
MnN1Ym9yZGluYWRhLmNybDBAoD6gPIY6aHR0cDovL2NybDIudWFuYXRhY2EuY29tL3B1YmxpYy9w
a2kvY3JsL0NBMnN1Ym9yZGluYWRhLmNybDAOBgNVHQ8BAf8EBAMCB4AwFgYDVR0lAQH/BAwwCgYI
KwYBBQUHAwgwHQYDVR0RBBYwFIESaW5mb0BldmjZXJlaWEuY2NtMA0GCSqGSIb3DQEBCwUAA4IC
AQDLXmTpUAfmTAQZvEN+ecztA2gnEXDq3UQE4h1QZt5egnP4OhvmXRfGWGbxtVwKz79fMXmyk
+Yv4iXPNYAYiG4Dv8dwKCYulU0jtxMqMlxwCTFtz+7ehi6snerb6F7to9s1QO2nFW1QkZ2s66CY2j
v0JzcbPdjrqGXQK3knL7bovFBoPh7ajmeCtBRDmXQrvUtFi8/qp6v4Fz/trwhJvE9kgEk6GNPWk8
EZeNfeIZLhLtV5OXA2BlaMmMbjMWzcLrMtxWBsd7HITFQjpaVrDeWzHE/uB2jA19ldr+vh5SnXr
8g5Y/tIl4IpqAzDWeaRH1I5vwDnIfWsLsoOmdqKNEFEoouE20vGDDDdBcUa6aYPb/D3ztB+bEK
yAg95BkBNijJswgsl3llwcQrpjrokdptJRI3ePlOZwYSIS9AiAcldusglY6HqX3WlzE+irEjMeND
AGMNuBgCGfACc9ANK/IbXmfmN0dzLhhmD4wWEIYxJnKcGOPpFgLK9kOklcpEs9ITsXZNyLfluvSL
r7vQ3fFNJ5kc7vkMujg7jAAZIryFPB9n3MIk83q0Gpz/du5FGUrOxchgNTpYOBMqRq+0ib88BVEb
CgWJ4sSO3JwlBzNWsKPjfv/ZwSlovNdtiXQMrsguXcpWX6RHBx1dUIDilt7Aq3QOc0c3cek5Qol
hg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA2 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVITSU-QE1B*

Subject OU: *EVICERTIA CLOUD QUALIFIED TSA QE1*

Subject O: *EVIDENCIAS CERTIFICADAS S.L.*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Wed Nov 20 11:29:24 CET 2019*

Valid to: *Sat Nov 20 11:29:24 CET 2027*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A3:F1:18:95:1B:02:FC:1C:DE:72:6D:BE:83:D8:3D:81:58:AB:B3:0B:8F:14:6D:34:8A:7B:88:CC:C5:2F:79:4A:4D:67:
93:AE:7A:55:31:2F:6D:6E:B0:91:99:8D:97:DC:13:E0:8C:0D:20:4B:13:E9:A2:A0:D4:00:1F:B1:06:D6:FE:C6:A6:C2:AE:41:38:0D:00:BC:2B:8F:08:DB:4B:6C:D8:D5:80:2C:02:16:6A:A7:A6:7E:E2:5E:DC:E5:DC:72:D1:5F:3
A:5C:BA:20:03:73:D4:35:7E:12:62:F1:EE:5C:B3:D9:EF:8F:02:BB:7C:02:7A:8D:0A:D0:BB:C3:C8:02:93:0B:0D:1F:FA:57:24:CC:30:13:F0:C2:53:2D:8C:12:E6:9E:05:31:29:A5:79:F7:0A:7E:E6:4A:B6:9D:F7:16:72:E4:7
E:61:11:13:BA:A6:7B:12:8E:34:BD:9C:61:7E:46:89:30:58:63:EA:65:E0:E7:94:00:C6:5D:14:E5:D0:8C:83:F3:DE:07:32:6F:75:13:C1:29:EB:22:DF:3D:B4:AB:98:AB:8F:EB:F1:63:4B:D1:AD:1B:CE:71:3E:D2:2A:CB:06:7E:2
9:CC:2F:66:87:28:05:AF:83:8E:86:12:11:C4:2E:3E:68:06:FE:EC:97:74:B7:5F:C6:DA:AF:47:02:03:01:00:01
```


Authority Info Access

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *26:95:95:24:2F:8A:90:E2:84:E3:F7:6B:E7:43:A3:47:3D:D0:24:DA*

Basic Constraints *IsCA: false*

Authority Key Identifier	*7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.47286.2.5* *CPS text: [Certificado de sello de tiempo electrónico.]* *CPS pointer: https://www.uanataca.com/public/cps/* *Policy OID: 0.4.0.2042.1.2*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl* *http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*
Extended Key Usage	*id_kp_timeStamping*
Subject Alternative Name	*info@evicertia.com*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*63:F3:67:59:42:A9:AB:49:5A:AA:5F:46:36:BD:FE:60:EA:7A:98:68:A9:6C:4A:5B:A5:34:2E:D8:F7:26:3B:5E*

X509SubjectName

Subject 2.5.4.97:	*VATES-B86021839*
Subject CN:	*EVITSU-QE1B*
Subject OU:	*EVICERTIA CLOUD QUALIFIED TSA QE1*
Subject O:	*EVIDENCIAS CERTIFICADAS S.L.*
Subject L:	*MADRID*
Subject C:	*ES*

X509SKI

X509 SK I	*JpWVJC+KkOKE4/dr50OjRz3QJNo=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-07-28T00:00:00Z

40 - TSP: EAD TRUST European Agency of Digital Trust, S.L.

.

TSP Name

Name	*[en]*	*EAD TRUST European Agency of Digital Trust, S.L.*
Name	*[es]*	*EAD TRUST European Agency of Digital Trust, S.L.*

TSP Trade Name

Name	*[en]*	*EADTrust*
Name	*[es]*	*EADTrust*
Name	*[en]*	*VATES-B85626240*
Name	*[es]*	*VATES-B85626240*
Name	*[en]*	*European Agency of Digital Trust, S.L.*
Name	*[es]*	*European Agency of Digital Trust, S.L.</*
Name	*[en]*	*EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*
Name	*[es]*	*EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

PostalAddress

Street Address	*[en]*	*Alba, 15*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28043*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Alba, 15*
Locality	*[es]*	*Madrid*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28043*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:info@eadtrust.eu*
URI	*[es]*	*mailto:info@eadtrust.eu*
URI	*[en]*	*https://www.eadtrust.eu/en/*
URI	*[es]*	*https://www.eadtrust.eu*

TSP Information URI

URI	*[en]*	*https://eadtrust.eu/en/*
URI	*[es]*	*https://eadtrust.eu*

40.1 - Service (granted): Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-NP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-NP*
Name	*[es]*	*Certificados cualificados emitidos por EADTrust RSA 2048 SubCA For Qualified Certificates 2019-NP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1081091677604567681 8*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGeDCCBWCgAwIBAgIJAJYIF4d0g4kSMA0GCSqGSIb3DQEBCwUAMIGcMUIwQAYDVQQDDDlFQURU
cnVzdCBSU0EgMjA0OCBSb290IENBIEZvciBRdWFsaWZpZWQgQ2VydGlmaWNhdGVzIDIwMTkxLzAt
BgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJF
UzEYMBYGA1UEYQwPVkFURVMtQjg1Nj2MjQwMB4XDTE5MDYwNjEwNTYyMVoXDTM1MDYwMjEwNTYy
MYowzbMxQDA+BgNVBAMMN0VBIFRydXN0IFTTQSAyMDQ4IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2Vy
dGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0
LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1Nj2MjQwMRcwFQYDVQQLDA5O
YXR1cmFsIFBlcnNvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPEz8MX8+TRSvmYq
S/OpZ6Voot0uD4eLdm4KzS/AFwdUAvzuu5ckSfNcwdjcP3wcoAIDP5PKLoPEmDQ+LABxKPzR+
lbTJw3MRoJMCxyd3FoZGnqorsVPH9SD8wM/ppNULtdW+K1WD6KTy6vwRJ+f4tLCW8/DmCFbOYYA
nAetATP5oCLdl5JU62DeKDj085n31q0STN2wu6B9bqLer85FuhpoIagGVMW4r4sGAhH8mLGCB+/o
+kNQLXENXmf/U8gSnfixB6QDRGuwS7i6QUnrig3O1fYYluPNJ4CqLnWwVGlML5AtCGQYFEIdE89/
xmQ9H/osuewN/tDzuqCAAuMCAwEAAaOCAqIwggKcMIGoBgNVHSAEgaAwgZ0wBgYEVR0gADCBkgYN
KwYBBAGDdQIBAQGDETCBgDAIBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBX
BggrBgEFBQcCAjBLDEITdWJvcmRpbmF0ZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkuIEV1cm9wZWFu
IEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0P
AQH/BAQDAgGGMB0GA1UdDgQWBBRr3pOyqvu62v7vRL7JZ9w9/nundTBjBgNVHRIEXDBagQ5jY1BI
YWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYYaHR0cDovL2NhLmVhZHRydXN0LmV1
hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRcMFqBDmNhQGVhZHRydXN0LmV1hhZo
dHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWFkdHJ1c3QuZXWGGWb0dHA6Ly9wb2xp
Y3kuZWFkdHJ1c3QuZXUwHwYDVR0jBBgwFoAUH99RtsGOGDAsjEJuM9i16HRQxKSkwSQYDVR0fBEIw
QDA+oDygOo Y4aHR0cDovL2NvbC5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXZeY TlwNDhlYWRx
MjAxOS5jcmwweAYIKwYBBQUHAQEEbDBqMEMGCCsGAQUFBzAChjdodHRwOi8vY2EuZWFkdHJ1c3Qu
ZXUvZWFkdHJ1c3Qtcm9vdC1yc2EyMDQ4ZWFkcTlwMTkuY3J0MCMGCCsGAQUFBzABhhodHRwOi8v
b2NzcC5lYWR0cnVzdC5ldTANBgkqhkiG9w0BAQsFAAOCAQEAdBpKcP8Acq/FqeeytxZPPJpJ78Ey
gU/mfJoSmt4KSmQ8ctG8kBKd+ZQp7z3bsfxywSbRXJjbFXq/ulzXBbCTTrw6jWvCF6HbQKBdv6pE
8g6vw3h/Zv2QB48PjbcJx8pyTos6bd8qTb99m5XPZPdx5pxQv6gjZ33seizHpsOv+PvCXRIQ65On
vbrNIZpgmteqAb/Uj7swKuW2TkF7jcadbsA1tb5W7Vs2D1Jf+FvWx4asqpCCOd8Ec1LBiaVeQ3fz
P41/Se/p1E3YhqlAckr8hGmz4ILCNkssePtORbFdR3jb4FtUcka3JrUxJgQ0PEk2lCdWrtRr1ywK
VaIDWs0E3w==

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA256withRSA*
Issuer 2.5.4.97:	*VATES-B85626240*
Issuer C:	*ES*
Issuer O:	*European Agency of Digital Trust, S.L.*
Issuer CN:	*EADTrust RSA 2048 Root CA For Qualified Certificates 2019*
Subject OU:	*Natural Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust RSA 2048 SubCA For Qualified Certificates 2019*
Valid from:	*Thu Jun 06 12:56:21 CEST 2019*
Valid to:	*Sat Jun 02 12:56:21 CEST 2035*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F1:33:F0:C5:FC:F9:34:52:BE:66:2A:4B:F3:A9:67:A5:68:A2:D3:AE:0F:87:8B:76:6E:0A:AF:3F:00:17:07:54:02:FC:E E:BB:97:24:48:82:0D:73:07:63:C4:FD:F0:72:80:25:0E:D3:F9:3C:A2:E8:3C:49:E2:0D:0F:8B:00:1C:4A:3F:34:7E:21:B4:C9:C3:73:11:A0:93:02:C7:27:77:16:86:46:AE:2A:A8:AE:C5:4F:1F:D4:83:F3:03:3F:A6:93:54:2E:D7:5 6:F8:AD:56:0F:A2:93:CB:AB:F0:44:9F:9F:E2:D2:C2:5B:CF:C3:98:21:5B:39:86:00:9C:07:A2:01:33:F9:A0:22:DD:97:92:54:EB:60:DE:28:38:F4:F3:99:F7:D6:AD:12:4C:DD:B0:BB:A0:7D:6E:A2:DE:AF:CE:45:BA:1A:68:25 :A8:06:54:C5:B8:AF:8B:06:02:11:FC:98:B1:82:07:EF:E8:FA:43:50:2D:71:0D:5E:67:FF:53:C8:12:9D:F8:B1:07:A4:03:44:6B:B0:4B:B8:BA:41:49:EB:8A:0D:CE:D5:F6:18:96:E3:CD:97:80:AA:2E:75:B0:54:69:4C:2F:90:2D: 08:64:18:14:42:1D:13:CF:62:C6:64:3D:1F:FA:2C:B9:EC:0D:FE:D0:F3:BA:A0:80:02:23:02:03:01:00:01*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*6B:DE:93:B2:AA:FB:BA:DA:FE:EF:46:4E:C9:67:DC:3D:FE:7B:A7:75*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*1F:D4:6B:B0:63:86:0C:0B:09:8C:42:6E:33:DD:7A:1D:14:31:2B:99*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crt* *http://ocsp.eadtrust.eu*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *82:34:0E:A4:D7:AC:D8:0D:F9:7D:C7:59:8C:94:95:58:8C:C8:87:3E:C9:50:6D:AD:0C:11:EA:11:94:33:39:9D*

X509SubjectName

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 2048 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *a96Tsqr7utr+70ZOyWfcPf57p3U=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

40.2 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Certificates 2019- NP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Certificates 2019-NP*
Name	*[es]*	*Certificados cualificados emitidos por EADTrust RSA 4096 SubCA For Qualified Certificates 2019- NP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5221470104002769698*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIdzCCBl+gAwIBAgIISHZjZSJoMyIwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNVBAMMOUVBRFRy
dXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZpY2F0ZXMgMjAxOTEvMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVT
MRgwFgYDVQR8DA9WQVRFUy1CODU2MjYyNDAwHhcNMTkwNjA2MTA1NjM1WhcNMzUwNjAyMTA1NjM1
WjCBszFAMDMGA1UEAwwJRUFEVHJ1c3QgUNBIDQwOTYgU3ViQXEgRm9yIFF1YWxpZmllZCBlDZX0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3Qs
IFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQR8DA9WQVRFUy1CODU2MjYyNDAxFzAVBgNVBAsMDk5h
dHVyYWwgUGVyc29uMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv4Lh3uZWD1QyEEpj
SrPdYiZSdYY8BqFrx2lnNledk8qBR9/8AXxt1R2AmgesDdVXQPCg3bRr+hxaY+fsIWkydknTZTj
XEy9dxXd9Z0MPlRL13A9oZNkFLuQcu/qq19bLV1igRWGwgRJXPyY9T0rAdShfO+1pun5UXRlZAsj
tFBM8FCQUu+8g0yEhRf8yJfjhlaQvTRCtt6305aBsUwyjkSSZI10L3IxgUCs9Kzv2iQXn8teB6Gs
c38OBpgDT3lppS1grRUwzc3nIYw7+NisRxMvyZ0xCdyMI24+PgZ99fKGzDlkOoKwIJLLUa3ecxgA
4xsIkcqJ5cd4PfbJnUuRoWsp6MO7Z9L09MHAl8IFUrv6ySq05aQORm3qLqOXCUO+A6B7EVzI5VtQ
ZcZsS713G9u5QIA5xA28KAuqxpIqSEAXWsDunx3j5KKvObIZjVD1i1PcXupqn2VoANphS2PHR1pk
JlkTbQFoYmEz7pw6VSz4rCMp1tE6uwHKPyehXBUenIEbHLyOWIXUEd4teNUB+WZpEFC7RyLYdJRK
jfpNXC++shc4tSsmBzH6CRWcdyxEbgNfaL V82xCGk0wY9OXsQfQZMqAAE/kYDCZelKr5GUh/DR8
SdHet9EaBT92AspFkBvBHoeE2qU1yMG/1X9upNq44P+z3t1aQ8z0m7GOJ7UCAwEAAaOCAqIwggKc
MIGoBgNVHSAEgaAwgZ0wBgYEVR0gADCBkgYNKwYBBAGDdQIBAQGDETCBgDAIBggrBgEFBQcCARYZ
aHR0cDovL3BvbGljcS5lYWR0cnVzdC5ldTBXBggrBgEFBQcCAjBLDEITdWJvcmRpbmF0ZSBDZXJ0
aWZpY2F0ZSBBdXRob3JpdHkuIEV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwu
MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBQGM9orzumBUU9p
3c3Ir98sLz2+XiBiBgNVHREXDHagQ5YUIbIYWR0cnVzdC5ldYYWaHR0cDovL3dJdyS0YWR0cnVz
dC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMG
A1UdEQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d5LmVhZHRydXN0LmV1hhVodHRwOi8v
Y2EuZWFkdHJ1c3QuZXWGGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwHwYDVR0jBBgwFoAU48Iw
NfcDw A8XsmOwUBPlFLEMWfQwSQYDVR0fBEIwQDA+oDygOoY4aHR0cDovL2NvbCS1YWR0cnVzdCSl
dS9lYWR0cnVzdC1yb290LXJzYTQwOTZlYWRxMjAxOS5jcmwweAYIKwYBBQUHAQEEbDBqMEMGCCsG
AQUFBzAChjododHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFkcTIw
MTkuY3J0MCMGCCsGAQUFBzABhhododHRwOi8vb2Nzcc5lYWR0cnVzdC5ldTANBgkqhkiG9w0BAQsF
AAOCAgEAcpyuo49fEIRPAe0YD9fdcJoBWGJmWWFuE3Gmu9nrzXy7IDISUk/UXZo7ogmpGesfaB219
gnlkZhlFTAQ4gEIW4yKCUwbyGefmhwwmcYoxz/Z9emWzRadrOUXGjO+bvvEFDr0Azbu0WOtR+aWwp
0H6RhUlyZPdTe+r26PskmPxAljbXLrb1JYYbfbEPX13u0jZBQm7BNjGcp5vgjJWTwRt5q8mA3RaK
hi1l+uv4E7prkO5CeSEdbwQz7aJo7snGw2RLO0RmvoPMQe+utRZMYNjWlEybfejvvFGcZ5yjLO
1iuqHVIO+TcZuC27zHgnB0t6XF79mNspslkcL9MA+7pmUTNLisqTKSVY6LXZjnudEReMc3q5zdR
vYYZAW1arUOMGFNwam/NJswxtPtCxh0Y3QhvBjxLOTzkP+ruxkoKhjUKLHIuW1bRqGlLg9CNGG14
Db16fvwUlyRRqaJH/aRKTZTgNHzRPt6gFxPO3q6Yly4TE/+odclqllrJNbth5FiqOt2D82WQjTKI
Gbgy+BgtdG40xh/BaXMVkxO8VjJHiETKpombbm6gUedEXhqFcXle3V3H8hoq0AS48Yld5GndkZJx
ww/pA7Hx2d9J1IggsP1QGdYC3fAtxCMB/RoeMklzgRIlG9mT5pkBK3epxZA+oEamXcIXzJLLzmCr
rerEILw=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 4096 Root CA For Qualified Certificates 2019*

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 12:56:35 CEST 2019*

Valid to: *Sat Jun 02 12:56:35 CEST 2035*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BF:82:E1:DE:E6:56:0F:54:32:10:4A:63:4A:B3:DD:62:26:79:75:56:3C:06:A1:63:C7:68:6F:36:5A:1D:93:CA:B4:47:DF:C8:F0:05:F1:B5:34:76:02:6A:A0:B0:37:55:5C:E3:C2:83:78:51:AF:E9:71:69:8F:9F:B2:55:A4:C9:F9:27:4D:94:E3:5C:4C:BD:77:15:DD:F5:9D:0C:3E:54:4B:23:70:3D:A1:93:64:14:BB:90:72:EF:EA:AB:5F:5B:2D:5D:62:81:15:86:C2:04:49:5C:FC:98:F5:3D:2B:01:D4:A1:7C:EF:B5:A6:E9:F9:51:74:65:64:0B:23:B4:50:4C:F0:50:90:52:EF:BC:83:4C:84:85:17:FC:C8:97:E3:86:56:90:BD:34:42:B6:DE:B7:D3:96:81:B1:4C:32:8E:44:92:66:5D:74:2F:72:31:81:40:AC:F4:AC:EF:DA:24:17:9F:CB:5E:07:A1:AC:73:7F:0E:06:98:03:4F:79:69:A5:2D:60:AD:15:30:CD:CD:E7:95:8C:3B:F8:D8:AC:47:13:2F:8D:9D:31:09:DC:8C:97:6E:3E:3E:06:7D:F5:F2:86:CC:32:24:3A:82:B0:20:92:CB:51:AD:DE:73:18:00:E3:1B:25:91:CA:BF:17:97:38:3D:F6:C9:9D:4B:BC:A1:6B:29:E8:C3:BB:67:D5:34:F4:C1:C0:97:C2:05:52:BC:3A:CB:9A:B4:E5:A4:0E:46:6D:EA:2E:A3:97:09:43:BE:03:A0:7B:11:57:49:E5:5B:50:65:E6:6C:4B:BD:77:1B:DB:B9:42:50:39:C4:0D:BC:28:08:AA:C6:92:2A:48:40:17:5A:C0:EE:9F:1D:E3:E4:A2:AE:39:B2:19:8D:50:F5:D6:23:DC:5E:EA:6A:9F:65:68:00:DA:61:4B:63:C7:47:5A:64:24:89:13:6D:01:68:62:61:33:EE:9C:3A:55:2C:F8:AC:23:29:D6:D1:3A:BB:01:CA:3F:27:A1:5C:15:1E:9C:81:1B:1C:BC:8E:5A:55:D4:11:DE:2D:78:D5:01:F9:66:69:10:50:BB:47:22:D8:74:94:4A:8D:FA:4D:5C:2F:BE:B2:17:38:B5:2B:26:07:31:FA:09:15:9C:77:2C:44:6E:03:5F:68:B5:7C:DB:30:86:93:4C:18:F4:E5:EC:41:F4:19:32:A0:00:13:F9:18:0C:26:5E:94:AA:F9:1A:52:61:FC:34:7C:49:D1:DE:B7:D1:2E:05:3F:76:02:CA:45:90:1B:C1:1E:87:84:DA:A5:35:C8:C1:BF:D5:7F:5A:A4:DA:B8:E0:FF:B3:DE:DD:5A:43:CC:F4:9B:B1:8E:27:B5:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: http://policy.eadtrust.eu

CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *06:33:DA:2B:CE:E9:81:51:4F:69:DD:CD:C8:AF:DF:2C:2F:3D:BE:5E*

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name

ca@eadtrust.eu

http://www.eadtrust.eu

http://ca.eadtrust.eu

http://policy.eadtrust.eu

Authority Key Identifier *E3:C2:30:34:47:03:C0:0F:17:B2:63:B0:50:13:E5:14:B1:0C:59:F4*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crl*

Authority Info Access

http://ca.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crt

http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *04:BF:1D:A6:D0:16:8B:DD:3F:2D:EC:2E:22:C5:0D:55:8B:DE:5C:7C:C9:51:6C:83:CB:63:93:35:2A:9F:0F:9C*

X509SubjectName

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *BjPaK87pgVFPad3NyK/fLC89vl4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

40.3 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP*

Name *[es]* *Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5842919634329022553*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIMdzCCCF+gAwIBAgIIURY4c0dWMFkwDQYJKoZIhvcNAQENBQAwgZwxQjBABgNVBAMMOUVBRFRy
dXN0IFTIQSA4MTkyIFVyb3QgRm9yIFF1YWxpZmllZCBDZXJ0aWZpY2F0ZXMgMjAxOTEvMC0G
A1UECzwmRXVyb3BlYW4gQWdlbmN5lG9mIERpZ20YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVT
MRgwFgYDVQRhDA9WQVRFUy1CODU2MjYyNDAwHhcNMTkwNjA2MTEyMDUxWhcNMzUwNjAyMTEyMDUx
WjCBszFAMD4GA1UEAwwJRUFEVHJ1c3QgUlNBIDgxOTIgU3Vi0lEgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5lG9mIERpZ20YWwgVHJ1c3Qs
IFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYyNDAxfzAVBgNVBAsMDk5h
dHVyYWwgUGVyc29uMIIEIjANBgkqhkiG9w0BAQEFAAOCBA8AMIIECgKCBAEAvdbc3AjQiIT7pjUs
7iwmyPFGJRP6OCW+Y3/+xPX7tK0EVbyCIFKoM7XX1Iwt2YJkO53r1v2MoCekjl9xGT3LHFlWAIHJ
x6IFzc0lwLfdeH/Ibt370XPg+szEa4cWtjtm8U0Aih9XHRD5d+0PnTG2PvjYrWE2wSUqqOnYUS
HPTWUY7DD3TZQFCTfBCbyVk8XCJbQxoFodBSnC+SSODzvkKzR1a2L4YyvDzL vtPIDJhgPNqWJmUyN
GayvVAkSQ8jxOn3C7XgtwvTmAFS+TJsO4mkmLSO3E9ausLHZVEVogqQdfqL1dFcOJFKUONqlcDv9
U80IS/D7DrgwBzUYz4Xx/lLVxmTk7A/7bu+qmnKi+y1NltKCMWMSQkZZMePwYGG/T82nxR4ln+A
yWYJWpMP93O0XP8/SMBk5d3xl+aNl5pdzTUPEKGQ8KjAF+HNfyZppFNpBEpXz9LRiTdQdcJHVpJ7
E7dwdfcIbM44YCzs8FZMLHxRAgfvwRKE1mWWR26HB+CqdqfC6IBkZ8Tl+2n6QwJ7UI26kv3dY9bCD
tWs4qu8BFjNngEEwQ8G/zOhlp50888TKnzZwZEYV6zasz/3l37hAHKhfi0ke6Kdh T0fERGvr1UBg
7jpmQNYzLHShOCs+Tq2qBwYIOEOIGFICaU/C7gvXKtzhyroqL8Gbz4L3VxsqlsVmre5KOzV5eEHhB
KjEF9KZFyBxDAwa65TNZcbSGGq3kc4NARUWdmkFMtQHF6GHUlxKexfQYPuUi3pFqwFG4SGxyPCcF
CGa0qfaCuIBKpcORKTvR+IbBAS8o+5N4eE8gqV1bnt0/vxzQ58DQn0QedEOY1jzAPVZzIq
2bmjVWdfeF3UJQ6XYKkMmUrabqKv5pBHPAFVbUptuOU0CK+1rY0UKWLWUJldgx+/TcnLK/vAne
vAcTdKyVqQzKCYKsv7ZwUxpZVUwAeJHMTpY0EnhbVzz/5JnHHNqyU937cyRfyOMGovQfhoNc/Rbk
bWwC0WY8+IAC41kBPSq64oA6Y5yKQizzogyp6+4WGHqyhhuR7OHi4IsXgSPOggI3oEfTs3UNzsX
yKi1bCQtyc4y0oHfbHBRuzaIRIP63FAhjy17AISH+BGlgDIzqgpknYbdaysAyQdwjPqfh6P36D80
FPF+WTIrTI7mUMLIfgTTJHWRFIcpC47Tkc+Tx3b/j5rb3Xs4d8jHLUDf4vzdowJGg2qdwJnGo0hk
bUa2PatYmaDktb70WgnHA/jV8+jPTz9ARgEcPY/IGS522KdVQrvE449EP33SMY/Mtb6Q2h6n+TUp
I5u8SLsvDPTugvwVU0WiUpp2te3wcY2xj7diV0gKwsx76sS7AvezdLisKQIDAQABo4ICojCCAp4w
gagGA1UdIASBoDCBnTAGBgRWHSAAMIGSBg0rBgEEAYN1AgEBAYMRMIGAMCUGCCsGAQUFBwIBFhlo
dHRwOi8vcG9saWNzLmVhZHRydXN0LmV1MFcGCCsGAQUFBwICMEsMSVN1Ym9yZGlnYXRlIENlcnRp
ZmljYXRlIEFIdGhvcml0eS4gRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4w
EgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFOqZz2sBGPmBRGn9
yJpordU303OYMGMGA1UdEgRcMFqBDmNbQGVbZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0
LmV1hhVodHRwOi8vY2EtZWFkdH1c3QuZXWGZWh0dHA6L y9wb2xpY3kuZWFkdH1c3QuZXUwYwYD
VR0RBFwwWoEOY2FAZWFkdH1c3QuZXWGFmh0dHA6L y93d3cuZWFkdH1c3QuZXWGFWh0dHA6Ly9j
YS5IYWR0cnVzdC5ldYYZaHR0cDovL3BvbGljeS5IYWR0cnVzdC5ldTAIBgNVHSMEGDAWgBQG5nPZ
U71Ap9FXjDZ/x+3Qed33yzBJBgNVHR8EQjBAMD6gPKA6hjhodHRwOi8vY3JsLmVhZHRydXN0LmV1
L2VhZHRydXN0LXJvb3QtcnVlbCDES MmVhZHEyMDE5LmVybD84BggrBgEFBQcBAQRsMCowQwYIKwYB
BQUHMAKGN2h0dHA6Ly9jYS5IYWR0cnVzdC5ldS9IYWR0cnVzdC1yb290LXJzYTgxOTJIYWRxMjAx
OS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1MA0GCSqGSIb3DQEBDQUA
A4IEAQBCe2VS5kD4qKddyF5XuTCAuyHeXXx9YUp3bnm+blEgSET/83BWUNcuwamsxPzkBhyeyvGn
8bNR0ncqo073Rlfai03qlXoo6K8jwVjwNuDzgtB4eYMBwvvKlmmuPRGd6q7dPWMw6boMa2KQcFXq
p0kp8F7yIY3agvt5wARRRMlK9Pgl+Fdd8xFpKRS2WFqONV4V3gIlhOuCjzUGKkTmsoH1DGJYwc3m
136bJe6kVLwFEEnqm28tvF86BygX11zUz9MnZx5obFGSGqdlcwWnQCGlNOL1052ovyCiQIOG6TE9
Lcs0PzcE9BqdWpxbGfnDK40U/05UCWDwIIa9qcSa4SWtrt6VEc5gtknnPVx07nYaFVY85IDNwz0L
xzWM6zMucx85F3jtxuhaA+s9E6qlxmFP8BnEiDnb7HtYAKPFg3Jf+FVToWoWRcKyD+c/t5pkOmtd+UCIAyMw
Iy25p33qTmw5yBwLdmjvtlZWynC6DwDx144KPYgc3j7+FVToWoWRcKyD+c/t5pkOmtd+UCIAyMw
nMExABku549pR/3RBB/WtYjSwCUNN3VlxN8fuPPTv89tGW+kZ3WO2o4cUsdZvM2du9eFYhGEsY0/
KpUUS17lsmeW+EKUPWzsopv5hlR6DXW/nj2bYrYp5A81hP8kk2sco8hIrKDqInHF6UhQDUbcYmFc
sKOmJFkC+xVRqQhFtB3o2CluNiC/NNw1WRVIKPv5gS0QOtzLvukLiL7uiyrHYP8OExHWSy+/+1n
bI5yiBuZc+bkITzbIbcmDSapr+yT3x56dip2x+SBMfrgDxVuU2j3cx/yudSvAseSx3e9PmyNRTca
6x2DZhcbAwIT8kZwJtjN0GCk8FoAYXmJuPD2XXaDWauYU2Tx1xb6OCol0OfThXxcx0Ai5MSC8QM
VIsN/1Zuyd14C+N4Z9mcZJcghH3gCaWodHA3lgQkTiVyhs7JHt0b/pemXmRfzxVI3hgP9FgmIYV
/YkDwdRbS9R3wuHY146RMUpKhHv5LK+fem163RuNthF7Cc+mrOczdIlrv6Gdd08nQlIAMMvIN0R
r6QmC8sp2A+rAMDxN2U6JZVccc/UB7I4RKin1z83Ta9uPjkXwikGts3BwbaH6IFUSY80wgqGRS
SeItaOlXjoH/IAqMEWaKpKzqtkap7Ir2JB6D9bw6Ke8yrVaiAZHCKaEFXzqwmJr0HnpLjrHJ2llu
4OcwtvDSEWBbbu+RjDc2T9+evbunu0Mtkh9Bb+OriFVyuYbSFhw2pdZcjdY6lQzA8C+/qsMH2Ln+
K6iDXGPGECC3+ASU5m7HscwhAGKJK+SgW1ZWW+ZxRh9s+lXxDATUrQotlFTxtQWKnU4FO4Clbo2a
cj1S

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 8192 Root CA For Qualified Certificates 2019*

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 8192 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 13:20:51 CEST 2019*

Valid to: *Sat Jun 02 13:20:51 CEST 2035*

Public Key:

30:82:04:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:BD:D6:DC:DC:08:D0:8E:54:D3:A6:35:2C:EE:2C:26:C8:F1:46:25:13:FA:38:25:BE:63:7F:FE:C4:F5:FB:B4:AD:04:55
:BC:82:20:52:A8:33:B5:D7:D4:8C:2D:D9:82:64:3B:9D:EB:D6:FD:8C:A0:27:A4:8C:8F:71:19:3D:CB:1C:57:D6:02:51:C9:C7:A2:05:CD:CD:25:C0:B7:DD:78:7F:DF:6E:DD:D3:D1:73:E0:FA:CB:59:11:AE:1C:5A:D8:ED:9B:
C5:34:02:28:62:F5:71:D1:0F:97:7E:D0:F9:D3:1B:63:F2:8D:8A:D6:13:6C:12:52:AA:8E:9D:85:12:1C:F9:7B:58:95:7B:0C:3D:FB:65:01:42:16:50:4E:C9:59:3C:5C:22:5B:42:8C:45:A0:14:A7:0B:E4:92:38:3C:EF:90:AC:D1:D5
:AD:8B:E1:8C:83:CC:BF:F2:B4:F2:03:7E:98:0F:D2:A5:88:99:4C:8D:19:AC:AF:54:09:12:43:C8:F1:3A:7D:C2:ED:78:2D:C2:F4:E6:00:54:BE:4C:9B:0E:E2:69:26:2D:2D:37:13:D6:AE:B0:B1:D9:54:45:68:82:A4:1D:B6:02:F
5:74:57:8E:24:52:94:38:DA:A5:70:3B:FD:53:CD:09:E7:F0:FB:0E:B8:30:07:35:18:CF:85:F1:FE:52:D5:C6:64:E4:EC:0F:FB:6E:EF:AA:9A:72:A2:FB:2D:4D:96:D2:0A:08:C5:8C:49:09:19:64:C7:8F:C1:81:86:FD:3F:36:9F:14:
78:96:7F:80:C9:66:09:5A:93:0F:F7:73:B4:5C:FF:3F:48:C0:64:E5:DD:F1:97:E6:8D:97:9A:5D:CD:35:0F:10:A1:90:F0:91:80:17:E1:CD:7F:26:69:A4:53:69:04:4A:57:CF:D2:D1:89:37:50:75:C2:47:56:92:7B:13:B7:70:74:47:D
B:33:8E:18:0A:2C:FC:15:93:0B:1F:14:40:81:FB:F0:44:A1:14:99:65:91:DB:A1:C1:F8:28:1D:AA:30:BA:94:1C:59:44:7F:9E:DA:7E:90:C0:99:7B:53:6E:A4:BF:77:58:F5:B0:83:B5:6B:38:AA:EF:01:16:33:67:80:41:30:43:C1:B
F:CC:E8:65:A7:9D:3C:F3:C4:CA:9F:36:70:64:46:15:EB:36:AC:CF:FD:C8:DF:B8:40:1C:A8:5F:8B:49:1E:E8:A7:61:4F:47:C4:44:6B:EB:D5:40:60:EE:3A:66:40:D6:33:2C:74:A1:38:2B:3E:4E:AD:AA:07:06:25:38:43:88:18:5
2:02:69:40:BB:82:F5:CA:B7:38:72:AE:8A:8B:F0:66:F3:E0:BD:D5:C6:CA:A5:B1:59:AB:7B:92:8E:CD:5E:5E:10:78:41:2A:31:05:F4:A6:45:C8:1C:43:03:06:BA:E5:33:59:71:B4:86:1A:AD:E4:73:83:40:45:45:9D:9A:41:4C:B
5:01:C5:E8:61:D4:23:12:9E:C5:F4:18:3E:EF:D4:DE:91:6A:C0:51:B8:48:6C:72:3C:27:05:08:66:B4:B6:A2:23:0A:E2:08:05:0A:5C:39:12:93:BD:1F:83:84:10:12:FE:5F:28:FB:93:78:AC:4F:20:A9:8D:61:9F:4F:FF:BF:1C:D0:6
7:9F:03:42:D7:F4:42:B7:44:41:85:23:00:FF:D5:66:B2:6A:D9:B9:A3:55:67:5F:78:5D:D4:25:0E:BF:5D:82:A4:32:69:49:AD:A6:EA:2A:FE:69:04:73:C0:15:56:D4:A6:2B:4E:53:40:8A:FB:5A:D8:D1:42:96:2D:65:09:95:D8:31:
FB:F4:DC:9C:B2:BF:BC:09:DE:BC:07:13:74:AC:95:A9:0C:CA:09:82:AC:BF:B6:70:53:1A:59:55:4C:00:78:91:CC:4E:96:34:12:78:5B:57:3C:FF:E4:99:C7:1C:DA:B2:53:DD:FB:73:24:5F:C8:E3:06:A2:F4:1F:86:83:5C:FD:16
:E4:6D:6C:02:D1:66:3C:F8:80:02:E3:59:01:3D:2A:BA:E2:80:3A:63:9C:8A:42:2C:F3:A2:0C:A9:EB:EE:16:18:7A:B2:86:1B:91:EC:E1:E2:E3:5B:17:81:23:CE:82:02:37:A0:47:D3:B3:72:3F:37:3B:17:C8:A8:B5:6C:24:2C:C9:
EE:32:D2:81:CF:77:80:51:BB:36:9F:44:83:FA:DC:50:21:8B:22:7B:02:54:87:F8:11:88:80:30:F3:AA:AA:64:9D:86:DD:6B:2B:00:C9:07:70:8C:FA:9F:87:A3:CE:E8:3F:34:14:F7:FE:59:FD:6B:B5:3B:7F:99:43:0B:20:88:13:4C:
91:D6:44:5D:5C:A4:2E:3B:05:CF:93:C7:76:FF:8F:9A:E1:FD:7E:1D:F2:31:CB:50:37:F8:BF:37:68:C2:3D:46:83:6A:9D:C0:9B:86:A3:48:A4:6D:46:B6:3D:A7:D8:99:A0:E4:7D:BE:F4:5A:09:C7:03:F8:D5:F3:E8:CF:4F:3F:40:
46:01:1C:3D:8F:C8:19:2E:76:D8:A7:55:42:2B:C4:E3:8F:44:3F:7D:D2:31:8F:CC:7D:BE:90:DA:1E:A7:F9:35:29:23:9B:BC:48:BB:2F:0C:F4:EE:82:FC:15:53:45:A2:52:9A:76:B5:ED:F0:71:8D:B1:8F:B7:62:57:48:0A:C2:CC:
53:EA:C4:BB:02:F7:B3:74:B8:AC:29:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*EA:99:CF:6B:01:18:F9:81:44:69:FD:C8:9A:68:AD:D5:37:D3:73:98*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*06:E6:73:D9:51:39:40:A7:D1:57:8C:36:7F:C7:ED:D0:79:DD:F7:CB*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crt* *http://ocsp.eadtrust.eu*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*20:02:B8:D5:AF:02:C5:A9:61:E1:0A:4D:A3:C2:7F:63:F3:5D:7F:7A:AD:94:15:99:DA:36:D5:2E:03:B7:A8:9D*

X509SubjectName

Subject OU:	*Natural Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust RSA 8192 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I	*6pnPawEY+YFEaf3Immit1TfTc5g=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

40.4 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019- NP

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019- NP*

Name *[es]* *Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Certificates 2019- NP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5004698788113163160*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIE5zCCBI2gAwIBAgIIRXRDCCFQ15gwCgYIKoZIzj0EAwIwgZsxQTA/BgNVBAMMOEVBRFRydXN0
IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmljYXRlcyAyMDE5MS8wLQYDVQQK
DCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAW
BgNVBGEMD1ZBVEVTLU14NTYyNjI0MDAeFw0xOTA2MDYxMTIzMTJaFw0zNTA2MDIxMTIzMTJaMIGy
MT8wPQYDVQQDDDZFQUR1cnVzdCBFQ0MgMjU2IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlmaWNh
dGVzIDIwMTkxLzAtBgNVBAoMJkV1cm9wZWFulEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwu
MQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1Njl2MjQwMRcwFQYDVQQLDA5OYXR1cmFs
IFBlcnNvbjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABIvhQDKEvOGURiGfC4WgrptHxeQsvHdo
1IcoQtGiOiEIyWoYs0vSbmIb9KUsPFb5s3bvFuNbDysIFO0PM5lF3yOjggKgMIKCnDCBqAYDVR0g
BIGgMIGdMAYGBFUdIAAwgZIGDSsGAQQBg3UCAQEBgxEwgYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9w
b2xpY3kuZWFkdHJ1c3QuZXUwVwYIKwYBBQUHAgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNhdGUg
QXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMB
AfBECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQMEFgQUw+LbEe82PGqASYsjRo07pzNr
mQwwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmbhdHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWh0
dHA6Ly9jYS5lYWR0cnVzdC5ldYYZaHR0cDovL3BvbGiljeS5lYWR0cnVzdC5ldTBjBgNVHREEXDBa
gQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRy
dXN0LmV1hhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFAFnmoTEmcaB7TxY
BHSvJKPXxENMEgGA1UdIfwRBMD8wPaA7oDmGN2h0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1
c3Qtcm9vdC1lY2MyNTZlYWRxMjAxOS5jcmwwdwYIKwYBBQUHAQEEazBpMEIGCCsGAQUFBzAChjZo
dHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MyNTZlYWRxMjAxOS5jcnQwIwYI
KwYBBQUHMAGGF2hddHA6Ly9vY3NwLmVhZHRydXN0LmV1MAoGCCqGSM49BAMCA0gAMEUCIGp+6oK3
2Ixu+fGongaszbcsuhvgfiZIGHNWQxtX44SN2AiEAjj8rAaWdPjX9KPDsCIj1yNY0UeE3heqjNssN
sXIzCVY=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withECDSA*

Issuer 2.5.4.97:	*VATES-B85626240*
Issuer C:	*ES*
Issuer O:	*European Agency of Digital Trust, S.L.*
Issuer CN:	*EADTrust ECC 256 Root CA For Qualified Certificates 2019*
Subject OU:	*Natural Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 256 SubCA For Qualified Certificates 2019*
Valid from:	*Thu Jun 06 13:23:12 CEST 2019*
Valid to:	*Sat Jun 02 13:23:12 CEST 2035*
Public Key:	*30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:8B:E1:40:32:84:BC:E1:94:46:21:9F:0B:85:A0:AE:9B:47:C5:E4:2C:BC:77:68:D6:57:28:42:D1:8E:FC:49:72:5A:86:31:D2:F4:BA:98:86:FD:29:47:8F:15:BE:6C:DD:BB:C5:B8:D6:C3:CB:22:05:3B:43:CC:E6:51:77:C8:E8*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*C3:E2:DB:11:EF:36:3C:6A:80:49:8B:23:46:8D:3B:A7:33:6B:99:0C*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*01:67:9A:84:C4:99:C6:81:ED:3C:58:04:74:AF:24:A3:D7:5E:41:0D*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc256eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc256eadq2019.crt* *http://ocsp.eadtrust.eu*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E5:F7:80:53:30:0C:16:9D:79:A7:FB:38:73:61:AD:2A:8D:1A:9B:B7:50:B9:18:3C:7B:B1:97:34:D5:42:F0:7C*

X509SubjectName

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 256 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *w+LbEe82PGqASYsjRo07pzNrmQw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

40.5 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Certificates 2019- NP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Certificates 2019-NP*

Name *[es]* *Certificados cualificados emitidos por ECC 384 SubCA For Qualified Certificates 2019- NP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *10391500411795310657*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIFJDCCBKugAwIBAgIJAJA2BpFoYohBMAoGCCqGSM49BAMDMIGbMUEwPwYDVQQDDDhFQURUcnVz
dCBFQ0MgMzg0IFJvb3Qg0QEgRm9yIFF1YWxpZmllZCBDZXJ0aWZpY2F0ZXMgMjAxOTEvMC0GA1UE
CgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMRgw
FgYDVQRhDA9WQVRFUy1CODU2MjYyNDAw1HcNMTkwNjA2MTEyMzE2WhcNMzUwNjAyMTEyMzE2WjCB
sjE/MD0GA1UEAww2RUFEVHJ1c3QgRUNDIDM4NCBTdWIDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmlj
YXRlcyAyMDE5MS8wLQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5M
LjELMAkGA1UEBhMCRVMxGDAWBgNVBGEMD1ZBVEVTLUI4NTYyNjI0MDEXMBUGA1UECwwOTmF0dXJh
bCBQZXJzb24wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAATZrnGktCAEuUZV2ZqHDfb7uiaQRwTpzALr
dQHT4DHCAuTGINfLfOldsdPkkVdMaVMbZmDz0BHfDZuJs1xEI6v4znSXh3Ib0mK7/0DNjtK1gfB
8BpRgQsbwLP1Vm42mD6jggKgMIICnDCBqAYDVR0gBIGgMIGdMAYGBFUdIAAwgZIGDSsGAQQBg3UC
AQEBgxEwgYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwVwYIKwYBBQUH
AgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kg
b2YgRGlnaXRhbCBUcnVzdCwgU y5MLjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIB
hjAdBgNVHQdEFgQUj7roZnJ0lkzM4lICDFzCx6bS4IwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3Qu
ZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWh0dHA6Ly9jYS5IYWR0cnVzdC5ldYYZaHR0cDov
L3BvbGljeS5IYWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBIYWR0cnVzdC5ldYYWaHR0cDovL3d3
dy5IYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hlodHRwOi8vcG9saWN5LmVhZHRy
dXN0LmV1MB8GA1UdIwQYMBaAFIgU/c7RCWBcdudnbiZIgcTqxJIBMEgGA1UdHwRBMD8wPaA7oDmG
N2h0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MzODRlYWRxMjAxOS5jcmww
dwYIKwYBBQUHAQEEazBpMEIGCCsGAQUFBzAChjZodHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1
c3Qtcm9vdC1lY2MzODRlYWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRy
dXN0LmV1MAoGCCqGSM49BAMDA2cAMGQCMH6bKBIXDD6FtWc0fgEKCr+eqz91zZc2lf6tW7kWgBB6
nXAR/iwpO52l3d7uDzP9SAIwf/zs2GCNsqLLLTaFiuk/pVy69WAhNqU/d/mL7Qh36ObWETT46WU/q
5PbcJlRDbMmC

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust ECC 384 Root CA For Qualified Certificates 2019*

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 384 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 13:23:16 CEST 2019*

Valid to: *Sat Jun 02 13:23:16 CEST 2035*

Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:D9:CE:B1:A4:B4:20:04:B9:46:55:D9:9A:87:0D:F6:FB:BA:26:90:47:04:E9:CC:02:EB:75:01:D3:E0:31:C2:02:E4:C6:20:D7:CB:20:E7:68:74:F9:24:B5:57:4C:69:53:1B:66:60:F3:38:11:DF:0F:6B:89:B3:5C:44:23:AB:F8:CE:D9:D2:5E:1D:C8:6F:49:CA:EF:FD:03:36:3B:4A:D6:07:C5:F0:1A:51:81:0B:1B:C0:B3:F5:56:6E:36:98:3E*

Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*8F:BA:E8:66:72:74:22:4C:CC:27:89:48:08:31:73:0B:1E:9B:4B:82*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*78:14:FD:EE:D1:09:60:5C:75:A7:67:6E:26:48:81:E4:EA:C4:92:01*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc384eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc384eadq2019.crt* *http://ocsp.eadtrust.eu*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F8:EA:34:65:13:55:C4:07:C9:03:87:56:08:B0:FF:A1:88:80:5E:93:08:1A:D0:3A:39:B8:22:6D:C3:5E:AD:B4*

X509SubjectName

Subject OU:	*Natural Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 384 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I	*j7roZnJ0IkzMJ4lICDFzCx6bS4I=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

40.6 - Service (granted): Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP*

Name *[es]* *Certificados cualificados emitidos por EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *8387960186886755879*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGdTCCBVZgAwIBAgIIdgFWUGBFicwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNVBAMMOUVBRFRy
dXN0IFJTQSAyMDQ4IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZpY2F0ZXMgMjAxOTEvMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVT
MRgwFgYDVQRhDA9WQVRFUy1CODU2MjYyNDAwHhcNMTkwNjA2MTA1NjIzWhcNMzUwNjAyMTA1NjIz
WjCBsTFAMD4GA1UEAww3RUFEYUH1c3QgUlNBID0wNDggI3VjQ0EgRm9yIFF1YWxpZmllZCBDZXJ0
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3Qs
IFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYyNDAxFTATBgNVBAsMDExl
Z2FsIFBlcnNvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPBQEUtUdXNGvxaYBi9k
1Tz3sYjYRwRLxCqLeOcUzE6adEvcTSVNMMzxu4hL+YSgzn+2WzIDSbjLKVTIUXIWGr1b3YzdYMyf
KaZw6m76MNO0gUm1BFS7catMHzvqkQJ9GBUF0hEecERo1SI9OeFltpXcmXK5d1cApNcbjQLDS7G
duRgDb6rgX+54yeLqb4opLsVEnYbO0umb5XXcO8m/tDhhUNqPWQZhUBubN3oPqdAM9CO5Q+nY2tV
qKp3HtC2W0Mc6rvUit1KtopIwVjvNDTnwSWxDdtpy5pWmA42Ko4+a5fRNDBJ55lT4FgPyjHsi5PZ
TtSIF60y38ys7feoMUCAwEAAaOCAqIwggKcMIGioBgNVHSAEgaAwgZ0wBgYEVR0gADCBkgYNKwYB
BAGDdQIBAQGD2ETCBgDAIBggrBgEFBQcCARY2aHR0cDov L3BvbGljcS5lYWR0cnVzdC5ldTBXBggr
BgEFBQcCAjBLDEITdWJvcmRpbmF0ZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkuIEV1cm9wZWFuIEFn
ZW5jcSBvZiBiEaWdpdGFsIFRydXN0LCBTLkwuMBIGA1UdEwEB/wQIMAYBAi8CAQAwDgYDVR0PAQH/
BAQDAgGGMB0GA1UdDgQWBBT62Qqiacv/aK/ymon/VpRUG7OZjzBjBgNVHRIEXDBagQ5jYUBlYWR0
cnVzdC5ldYWaHR0cDov L3Zkdy5lYWR0cnVzdC5ldYYYaHR0cDov L2NhLmVhZHRydXN0LmV1hhlo
dHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRw
Oi8vd3d3LmVhZHRydXN0LmV1hhVodHRwOi8vY2EuZWFkdHJ1c3QuZXWGGWb0dHA6Ly9wb2xpY3ku
ZWFkdHJ1c3QuZXUwHwYDVR0jBBgwFoAUH9RrsGOGDAxJjEJuM916HRQxK5kwSQYDVR0fBEIwQDA+
oDygOoY4aHR0cDov L2NybC5lYWR0cnVzdC5lZS9lYWR0cnVzdC1yb290LXJzYTIwNDhlYWRxMjAx
OS5jcmwweAYIKwYBBQUHAQEEbDBqMEMGCCsGAQUFBzAChjdodHRwOi8vY2EuZWFkdHJ1c3QuZXUv
ZWFkdHJ1c3Qtcm9vdC1yc2EyMDQ4ZWFkcTIwMTkuY3J0MCMGCCsGAQUFBzABhhdodHRwOi8vb2Nz
cC51YWR0cnVzdC5ldTANBgkqhkiG9w0BAQsFAAOCAQEAUI5MNqYKLh2Is3HPs6xy0E4AYTmWqdlv
NJRl9syz1Pcfz5UxTk24M7gzJ1wlC7f+syJIv8f8FNTCXKHnC S0tgDNTIVf3YhxvvBwxcXYTUP
zK1LTfe5sJ4cyaAE5c701XWZFPhicRxZCPN1vgjD5CMuHB31LwbDzda28kpuvv247+WudKbGXoHw
6dyM5MUEU0f4q7X/Tw+EiV917+zIcfCn5A9hS3RSYb023DrqKQkrQoH/zhoHEdBWdG1dCHMfy/no
x/RhISy5YCZyY38OhzIO1RB/i25hHsMBZpLjN673d3a2nsOQShUd/8socvS7/YbN09fOuEcSZIta
k8uZyA==

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA256withRSA*
Issuer 2.5.4.97:	*VATES-B85626240*
Issuer C:	*ES*
Issuer O:	*European Agency of Digital Trust, S.L.*
Issuer CN:	*EADTrust RSA 2048 Root CA For Qualified Certificates 2019*
Subject OU:	*Legal Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust RSA 2048 SubCA For Qualified Certificates 2019*
Valid from:	*Thu Jun 06 12:56:23 CEST 2019*
Valid to:	*Sat Jun 02 12:56:23 CEST 2035*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F0:50:11:4B:54:75:73:46:BF:16:98:06:2F:64:D5:37:B7:B1:88:D8:47:04:4B:CC:2A:8B:78:E7:14:CC:4E:9A:74:4B:DC:4D:25:4D:30:CC:F1:BB:88:4B:F9:84:A0:9B:ED:96:AC:90:D2:6E:32:CA:55:39:54:25:72:16:1A:BD:5B:DD:8C:DD:60:CC:9F:29:A6:70:EA:29:FB:E8:C3:4E:D2:05:26:D4:11:52:7F:B7:1A:B4:C1:F3:CA:A9:10:27:D1:81:50:5D:22:11:E7:04:46:8D:52:14:E7:85:96:DA:57:7A:65:CA:E5:DD:5E:02:93:5C:86:34:0B:0D:2E:C6:76:E4:60:0D:BE:AB:81:7F:B9:E3:27:8B:AA:1E:28:A4:BB:15:12:76:21:3B:4B:A6:6F:95:D7:70:EF:26:FE:D0:E1:85:43:6A:3D:64:19:85:40:6E:6C:DD:E8:3E:A7:40:33:D0:8E:E5:0F:A7:63:6B:55:A8:AA:77:1E:D0:B6:5B:43:1C:EA:BB:D4:8A:DD:4A:B6:8A:48:C1:58:EF:34:34:E7:C1:25:B1:0D:DB:69:CB:9A:56:98:0E:36:2A:8E:3E:6B:97:D1:34:30:49:E7:92:53:E0:58:0F:CA:31:EC:8B:93:D9:4E:D8:92:20:5E:B4:CB:7F:32:B3:B7:DE:A0:C5:02:03:01:00:01*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*FA:D9:0A:A2:69:CB:FF:68:AF:F2:9A:89:FF:56:94:54:1B:B3:99:8F*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*1F:D4:6B:B0:63:86:0C:0B:09:8C:42:6E:33:DD:7A:1D:14:31:2B:99*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crt* *http://ocsp.eadtrust.eu*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *29:40:0D:5D:52:0D:A0:85:2E:4D:D5:3A:5B:85:D3:26:8F:9A:3D:CC:60:61:C2:85:47:44:40:CB:85:9E:09:A8*

X509SubjectName

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 2048 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *+tkKomnL/2iv8pqJ/1aUVBuzmY8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

40.7 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Certificates 2019-LP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Certificates 2019-LP*
Name	*[es]*	*Certificados cualificados emitidos por EADTrust RSA 4096 SubCA For Qualified Certificates 2019-LP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7219277311459685234*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIldTCCBI2gAwIBAgIIZDAGdySXc3IwDQYJKoZIhvcNAQELBQAwgZwxQjBABgNVBAMMOUVBRFRy
dXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBDZXJ0aWZpY2F0ZXMgMjAxOTEvMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVT
MRgwFgYDVQR8bDA9WQVRFUy1CODU2MjYyNDAwHhcNMTkwNjA2MTA1NjU3WhcNMzUwNjAyMTA1NjU3
WjCBsTFAMD4GA1UEAwwJRUFEYHU1c3QgUlNBIDQwOTYgU3ViQ0IgRmByIFF1YWxpZmllZCBDZX10
aWZpY2F0ZXMgMjAxOTEvMC0GA1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3Qs
IFMuTC4xCzAJBgNVBAYTAkVTMRgwFgYDVQR8DA9WQVRFUy1CODU2MjYyNDAxFTATBgNVBAsMDExl
Z2FsIFBlcnNvbjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKsZ4po900I2BEfKsZB1
FhIgfjXksI/EDv+aj+Q8Qkdxhml/3XYjtr2vd2PrjUNrgECyuxz8ix9z90vEhz1wMWVRVRs10btEN
4Aw9qzSZrQyKewx5SY7Y7YSYa4P4SYrVZSWO/4RxLFcAec9Q4eM3owyuYFTfFyGHJE43hKu+THf
Hw0bghPyDjqGe+15/xh7JCdVlMc56kOU/tcKQd7ack3FQqiV9v+D+ki70f2E2pbUY1zhCvx9/vTA
POVOzQ9777lqzW0CsU51VnSjsxwphdX3HdTQot4FKY7/U72/oDQGajg6Dzd2awfBRQSLfASL1nfH
SLCo18vcEog9OM6G0uJ0dLK2gU+sCdFxSu6cle/UDpu6A4kfe7HHUKcJHmbhkkBtrXw55CdUSdym
mb6+c0brqotKiCBm2NPlNLGNAAwERW0N2gMmbgq13tQIY4FvGU9oIk1FzFiWpiP7ELOEAa+7f+3
YscaoQ7zlVvcZ17xF/gi/KnEEjB0UBL10K8naU61FXS0fakgG7JF0T15GSGDiNX/HE8p+0VOu6GO
KKoGtvkthgs+K1h66Hoa3sUA3aMo1IgMifOzwR7sfzkKttuTvDFRptvifx7/svtCjOu5k7sPxU4
vNgUL1rWIcwe9gIkgdf0p79+SjoBDAc+kPMIIMaSTAr4m70EdIWU1mBD3AgMBAAGjggKiMIICnjCB
qAYDVR0gBIGgMIGdMAYGBFUdIAAwgZIGDS6GAQQBg3UCAQEBgxEwgYAwJQYIKwYBBQUHAgEWGWh0
dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwVwYIKwYBBQUHAgIwSwxJU3Vib3JkaW5hdGUgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjAS
BgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHO4EFgQUMS5X72kv2esv2yA4
CeOEpyxJ/0UwYwYDVR0SBFwwWoEOY2F.AZWFkdHJ1c3QuZXWGFmbldHA6Ly93d3cuZWFkdHJ1c3Qu
ZXWGFWh0dHA6Ly9jYS5lYWR0cnVzdCSldYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdCSldTBjBgNV
HREEXDBagQ5jYUBlYWR0cnVzdCSldYYWaHR0cDovL3d3dy5lYWR0cnVzdCSldYYVaHR0cDovL2Nb
LmVhZHRydXN0LmV1bhlodHRwOh8vcG9saWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFOPCMDRH
A8AP7TjsFA75RSxDFm0MEkGA1UdHwRCMEAwPq A8oDqGOzbhldHA6Ly9zcmwuZWFkdHJ1c3QuZXUv
ZWFkdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFkcTlwMTkuY3JsMHgGCCsGAQUFBwEBBGwwajBDBggrBgEF
BQcwAoY3aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNhNDA5NmVhZHEyMDE5
LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFkdHJ1c3QuZXUwDQYJKoZIhvcNAQELBQAD
ggIBAB5p4UlcQ5K3+sw0s2TPQLbleanJmCEcMjqNkv4wpxndMXcK16x7qkZwtp/vW6u8Ohp7eRR
2pmQwbhb4vFT11GeHGxSDF6Nhj71K5xy7lYL/P4etc5P12MlycKAtdFPSJoN1+utmXhADZQ4r65
riNTwhJHCqq3abXd13IkoJzqouqOpy8ndFY5tuVDMXU9ih4l1gV5dMs2pVgre/gS7U4nPA3OFRSV
mxZR+u7Q6YPmXoq06iG5F6uAhQGibiaUf4pUYcT1TQFx5hLSEMfHs2fwkFs70YBFwIVdpDSpWLie
YtZfpKvQcOWWpCIwujktuOzBfUWBi0ohm9Qu6ydw+2MUVFcZcqRTC/Fn9UqAIFylJMT0F5hvZ4w9
YvqsB1XI2taPg1dMgM5TvXa41pjPAqN7+1BgtDH0gtEmERpQpbbfLLCYu/uoVn25ZoEr6SKSCfB
V1MFRr7Fm0G23x5vARR82cHfOVF4c8MVAsfCKJZKmirQLLed8cSMPB4pkFRtKPkXPjs8RsHLBOQ
ONt9pNm/DVSD7xweY+qqfoHEiD3vNqiQXTFvUNlkcbhAGZqAMZC2GGejoASNq9VQACu6vNww1nd/
CPIlPPPCnJKPKLbYQPWqndA24K9ZIrpOECg0YGfqxW5mbv4uWD5dAYC/bokXPcZxajyveVNwq7sh
ndsX

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 4096 Root CA For Qualified Certificates 2019*

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 12:56:57 CEST 2019*

Valid to: *Sat Jun 02 12:56:57 CEST 2035*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AB:19:E2:9A:3D:D3:47:F6:04:47:CA:B1:90:75:16:19:48:81:FA:97:92:C5:04:0E:FF:9A:8F:E4:12:42:47:71:86:65:37:5D:82:20:B7:6B:DD:D8:FB:63:50:DA:E0:94:2C:AE:C6:BF:22:C7:DC:7D:D3:21:21:CF:5C:0C:59:54:55:46:CD:74:6E:D1:0D:E0:0C:3D:AB:34:99:AD:0C:8A:7B:0C:79:49:8E:D8:ED:84:98:6B:83:F8:49:8A:D5:65:25:8E:FF:84:71:2C:57:00:79:CF:50:E1:E3:37:A3:0C:AE:60:54:DF:14:5C:86:1C:91:38:DE:12:AE:F9:31:DF:1F:0D:1B:82:13:F2:0E:3A:86:7B:ED:79:FF:18:7B:24:27:55:94:C7:39:EA:43:94:FE:D7:0A:41:DE:DA:72:4D:C5:42:A8:95:F6:FF:83:FA:48:BB:D1:FD:84:DA:96:D4:63:5C:E1:0A:FC:7D:FE:F4:C0:3C:E5:4E:CD:0F:7B:EC:8A:B3:5B:40:AC:53:9D:55:9D:28:EC:C7:0A:61:E1:72:37:1D:D4:D0:A2:DE:05:29:8E:FF:53:BD:BF:A0:34:06:6A:38:3A:0F:37:76:6B:07:C1:45:04:8B:7C:04:8B:D6:B7:C7:48:B0:A8:D7:CC:9C:12:88:3D:38:C8:86:D3:02:74:74:BF:36:81:4F:AC:09:D1:71:4A:36:BA:72:57:3F:B4:3A:5A:E8:0E:24:7D:E4:C7:1C:93:9C:1E:66:E1:92:40:6D:B5:7C:39:E4:27:54:49:DC:A6:99:BE:BE:73:46:EB:AA:8E:4A:88:20:66:D8:D3:C8:36:D2:C6:34:00:30:11:15:B4:37:68:0C:99:B8:2A:D7:7B:50:95:8E:05:BC:65:3D:A0:89:35:17:31:5F:5A:98:8F:EC:42:CE:10:06:BE:ED:FF:B7:62:C7:1A:A1:0E:F3:95:5B:DC:67:5E:F1:17:F8:22:FC:A9:C4:12:30:74:50:12:F5:D0:AF:27:69:4E:B5:15:74:B4:7D:A9:20:1B:B2:45:D1:3B:79:19:21:83:88:D5:FF:1C:4F:29:FB:45:4E:BB:A1:8E:28:AA:06:B6:F9:2D:86:0B:3E:2B:58:7A:EA:D1:E8:6B:7B:14:03:76:8C:A3:52:20:32:27:CE:CF:04:7B:B1:FC:E4:2A:DB:6E:4E:F0:C5:46:9B:6F:89:FC:7B:FE:CB:ED:0A:33:AE:E6:4E:EC:3F:15:38:BC:D8:14:2E:D5:87:73:07:BD:82:59:20:75:FD:29:EF:DF:92:8E:80:43:01:CF:A4:3C:C2:08:31:A4:93:02:BE:26:EF:41:1D:95:65:35:98:10:F7:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: http://policy.eadtrust.eu

CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45*

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name

ca@eadtrust.eu

http://www.eadtrust.eu

http://ca.eadtrust.eu

http://policy.eadtrust.eu

Authority Key Identifier *E3:C2:30:34:47:03:C0:0F:17:B2:63:B0:50:13:E5:14:B1:0C:59:F4*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crl*

Authority Info Access

http://ca.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crt

http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7F:D0:FF:DF:3A:A0:C9:69:93:DC:6D:1A:DA:D7:79:22:63:81:AC:7B:5C:48:A0:1D:1A:2E:4A:FC:6C:2F:77:7A*

X509SubjectName

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I	*MS5X72kv2esv2yA4CeOEpyxJ/0U=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

40.8 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019-LP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019-LP*
Name	*[es]*	*Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Certificates 2019-LP*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*1106346666635777153*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIMdjCCCF6gAwIBAgIJAJnJVFEJM1SBMA0GCSqGSIb3DQEBDQUAMIGcMUIwQAYDVQQDDDlFQURU
cnVcqC7BSL0lEgODE5MiBRb290IENBIEZvciBRdWFsaWZpZWQgQ2VvdGlmaWNhdGVzIDIwMTkxLzAt
BgNVBAoMJkVlcm9wZWFuIEFnZWNjeSBhZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJF
UzEYMBYGA1UEYQwPVkFURVMtQjg1Nj12MjQwMB4XDTE5MDYwNjExMjMwMVoXDTM1MDYwMjExMjMw
MVowgbExQDA+BgNVBAMMN0VBRFRydXN0IFJTQSA4MTkyIFN1YkNBIEZvciBRdWFsaWZpZWQgQ2Vy
dGlmaWNhdGVzIDIwMTkxLzAtBgNVBAoMJkVlcm9wZWFuIFFnZWNjeSBhZiBEaWdpdGFsIFRydXN0
LCBTLkwuMQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1Nj12MjQwMRUwEwYDVQQLDAxM
ZWdhbCBQZXJzb24wggQiMA0GCSqGSIb3DQEBAQUAA4IEDwAwggQKAoIEAQC9wXqa6r1OTC51CZW
Z7o0Ct9DqsMnWyxQzymidI2S43S4C/ddEipUG7/CndjP12gZjHK7JbED+bytEWClqRQAc+ttIptj
EBy+wHwkaHKD7qucawvJqS0fie2tPhuwpF/1sZ4XmSckaw3R0H1lKOzcMrgdvXeB9BWe0HNFKa
pcMBxXrvUd5bh6u16saSkWC51YKuRrfMuR7FWYA7pcHFjDnzSnzJhaBQ1Z7QGvRdvrrS52L88rqd
B7LCSKleNjnkORaQ0GQtRqXhxnggFHi7BlQNhuZ84Evhm4nZ3vjGPGPMBzhwHiU08sTh4nD3doY
ymOyn9+DkF7mrXj71sJaNPId9in9R0KViurbjUhl1JNBulu4zs2pNRWM6GAgx7Pdcv85dPpWF0j
GZTFqx8pKJskdrmy/CngKMHMDCss7YOjMoqx5Pwk2nFPxC6PynFmTGAbY09w68SQoRVY2Eh9MBM1
CzDnvMj+IT7IoRLsuKV9uCRxwX1NfzPxTRqSMXIdm8MZcpoCs2XLXuQSUP4f5zyWlVEplCMzCGV
4E6T3Obl2mACx+tOx9mDayor0DmWwfE2bbCwNoOtK8S/ZvOVdTPPLF/5b1nNnwhKxe+62UwYBWnY
qAN2YNbUJuFjjmk2uOuYX0AyQACmxJzKPS+Chtzpel++dlw5/gH2sSm4x287T2ZQKl13kqKTC0tEH
IDo9/b+Zpr7/H69my3Jh14VKSHgcBB3yAZanHbnbjSUNCgvcqESCtQ/KxxHgkQP2RcbRuMaRLNxj
WwgeycOBnv1+Tdo7mlorNbj53bW6N0LSjEZOiZJobTbIP19vB6CuaF5nT0LuKt2gek0BK0zqcO
PhBcPEY9uSclTMJO0P7wfArzZ60Jtf/hBjLrLKRoCvAkxureCPCh3EF7v0xjrXEYSgXktq4uUBtW
0HeUsBrgY/T8mlKIB9vzlxLT7NdwPsPyolsQEHeYOOuIe8yQHs/u1Elro32bHHauxqmmmkOKSC4V
linKOhdrLr9N4K825QewzkPKK0Ki8E5zCOzFVIseas6OHc/e/PHPXhNQyGJpkMyCeYXzMS6bXf49
4pRtKJFBX6A+v+L9cp2/4/6ycj6WHphiMoQ2aHM4OnBjKI1xSvPw+aXbRFAsHeq1B7DHIC2gv4S
6U1VJgZJYjlcQBbbPwthK Y8Ibz5GhuLDsfj7HoE1FoSivv7BOAp8pdYmhU+MeQZ1JQTB0GtuhyG
c5pJldnnvKvyxDoNAVN9+wIXYSnDwwgYjNKa41PP8IwaEkMkyP60guJaZWZsIP8Xh/T+CLWWAMVf
gHjhIAaxD13wvE4X18QGIVGiZo4QEZnWb21AzUFlIyJ4es3i046aXETAgMBAAGjggKiMIICnjCB
qAYDVR0gBIGgMIGdMAYGBFUdIAAwgZIGDSsGAQQBg3UCAQEBgxEwgYAwIQYIKwYBBQUHAgEWGWh0
dHAtcy9wb2xpYXkuZWFkdHI1c3QuZXUwVkYIKwYBBQUHAgIwSxwJUVib3JkaW5hdGl/gQ2VvdGlm
aWNhdGUgQXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjAS
BgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUjEj9L8KVkDKzpNd
ej0m2BSUps8wYwYDVR0SBFwwWoEOY2FAZWRkdHJ1c3QuZXWGFmh0dHA6Ly93d3cuZWFkdHJ1c3Qu
ZXWGFWhldHA6Ly9YSSYWR0cnVzdC5ldYZaHR0cDovL3BvbGlpSSIYWR0cnVzdC5ldTBjBgNVHR
HREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYvaHR0cDovL2Nh
LmVhZHRydXN0LmV1bhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MB8GA1UdIwQYMBaAFAbmc9lR
OUCn0VeMNn/H7dB53flLMEkGA1UdHwRCMEAwPqA8oDqGOGh0dHA6Ly9cmwuZWFkdHJ1c3QuZXUv
ZWFkdHJ1c3Qtcm9vdC1yc2E4MTkyZWFkcTIwMTkuY3JsMHgGCCsGAQUFBwEBBGwwajBDBggrBgEF
BQcwAoY3aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNhODE5MmVhZHEyMDE5
LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFkdHJ1c3QuZXUwDQYJKoZIhvcNAQENBQAD
ggQBALUKGYkyYwhrLkXj1rsoSmnNWd5GlzOS2j2H7i4/4mu1qExONAedUXXM0PHiXkmAehuXNzMR
kXsFvRxu0Ps3F7Q+WnIJ53vQnrVMKzk0udpyuXZ9tkm0J2PsVJ0l0+cPnSTD9MSC/TI9K95UMC
E+Ct0Ene9g9nFSaPL4Y5b6IVyUPV9EecGNpYjpRMnf9bBH+IC5+oxpAVCmoT4GqHkDPrvYbdbGX6
TQ5GXv4UnQVImN0mNgGE6uhDeG6zn8HhglFkpvsPRBRfDSKnmvjXg0HPBsVUUjUMFboGy0J9ZHyK
hv+/260D89Gmj4CwmI7mdHP04pCDMrIcKYHsH4FvLQP3Wp2uVwWWvA3A6eDPcsVXFdFEOZrjitms
ArWNpAjUlkfj+DpYRAcYh6wsWM7mzVbp1TaI2vz1RKsqkpbKnuGaD8jtUx49YV9+HInAICuX1z
483fRdzp94MzfuY/vGZxopY81JypASJ2gQ7I3Dut7EzkCOTXNcSjcVXhFVuSFMR9+dMdBz1
TX1dHvw8BtwEhGkvtGHkdMIX+2AKw3Nan89fZPK1r8n0oRaFufiE7uRAMSDmPVISThyWds81K0NX
04j7im47wpS41VOIGvXHWYNRN24y+jSkqtCtFbxryFXsaQKVNm77zwjSm+zTvPBJVo2JLX7itPxo
9vYCDyLtMR6oboF4GYYV1YdSqJRdRoMMApRjdHhOwGktUZ9GgDqvRElFIDa85kf+cOuXKFU9eTH
tg5HLLhUtplq+GZGIYIt8XV0IoZpUQQmf3zSuJQc/0OUduTaKsybDBntYjQUrtM1Tzlj6QPG7Tb3
MGkF6sdL GlMFE8KeUosIEKJyvcDtHDuvJv4CuqNEZuR6pP8T29xvl+JcTBcb8boPKioo2f0tLUOf
2SpT+hNnBVrPwKetZyFZPAkxwhYrX/z7DyVK95s+vzoWH/tmNSDIH97wdTOONfQfgR80B2RpZ6bp
N5TCxX2lKyKdA4DpPk3nV15Z3oG9MtYFMYb18ZsQedpZYPhKrSRjtG+ZnRYLiY7H/4nRX1cIL25p
VQu6hbvFgQ5sHXQKGXcatTxCIL8vFMduIbS19benlgkoi9UQIcu4vTTR87Ti/sWX9IB7KVIApInV
KaE98xm9o2FQBROiyFeLf5KyLOLXA0e1BKOu2BOepOeDpX7dr4EhF4806m8Eu7qb4eNuQ8xyuXu9
pD9+3TH8czvN4WJVq466BYE/NlCWPxTcB1oqx56NlvGGgn74LZVMbHb8BkSBlNeGmEXAia+IauAB
uYZNE+OcVDh3TjiSZi1GU0auCzbilwp/Zr1xM+VPaG1AWoWcVv7rQ+bAVw78nULnJQNPRIoK9gkv
ZOA=

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 8192 Root CA For Qualified Certificates 2019*

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 8192 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 13:23:01 CEST 2019*

Valid to: *Sat Jun 02 13:23:01 CEST 2035*

Public Key:

30:82:04:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:BD:C1:7A:9A:EA:B2:22:39:30:B9:D4:26:56:67:BA:34:0A:DF:43:AA:C3:27:5B:2C:50:CF:29:AD:74:8D:92:E3:74:B
8:09:F7:5D:12:DA:54:1B:BF:C2:9D:D8:CF:D7:68:19:8C:72:BB:25:B1:03:F9:BC:9F:11:60:A5:A9:14:00:73:EB:6D:22-9B:63:10:1C:BE:C0:7C:24:68:72:83:EE:AB:9C:6B:08:C9:A9:2D:1F:89:ED:9F:3E:18:89:C2:91:7F:D5:F
B:19:E1:79:92:7A:46:B0:DD:1D:07:97:52:B4:CD:C3:2B:81:DB:D7:78:1F:41:59:ED:07:34:52:9A:A5:C3:01:C5:7A:EF:51:DE:61:D2:EE:B5:D2:C6:92:91:60:B9:D5:52:B1:46:B7:CC:B9:1E:C5:59:80:3B:A5:C1:C5:8C:3C:59:
9E:E:C6:61:68:14:35:27:6E:D0:1A:F4:5D:AE:FA:D2:E7:62:FC:F2:BA:9D:05:32:C2:48:A9:5E:36:39:E4:39:16:90:D0:64:2D:46:A3:E1:C6:78:20:14:78:BB:06:54:0D:86:E6:7C:E0:4B:E1:9B:89:D9:DC:9B:E3:18:F1:8F:30:1C:E
1:C0:78:94:D3:CB:13:87:89:C3:DD:DA:18:CA:63:B2:9F:DF:83:90:5E:E6:AD:78:D3:D6:C2:5A:34:73:C8:77:D8:A7:F5:1D:0A:56:2B:AB:6E:35:21:23:52:4D:06:E2:2E:E3:3B:36:A4:D4:56:33:A1:80:83:1E:CF:75:CB:FC:E5:
D3:E9:58:5D:23:19:94:C5:AB:1F:29-28:9B:24:76:B9:F2:FC:29:E0:28:C1:CC:0C:2B:2C:ED:83:A3:32:8A:B1:E4:FC:24:DA:71:4F:C4:2E:8F:CA:71:66:4C:60:21:63:4F:70:EB:C4:90:A1:15:58:D8:48:7D:30:13:35:0A:B0:E7:B
C:C8:FE:7F:5E:D3:A3:F4:AB:B2:E9:15:F6:E0:91:C7:05:F5:35:FC:CF:C5:34:6A:48:C5:C8:76:6F:0C:65:C8:E8:0A:CD:97:2D:7B:90:49:43:F8:23:9C:F2:5A:55:44:A4:80:8C:CC:21:95:E0:4E:93:DC:E6:ED:DA:60:02:C7:EB:4
E:C7:D9:83:6B:2A:2B:D0:39:96:C1:F1:36:6D:B0:B0:36:83:AD:2B:C4:BF:66:F3:95:75:33:CF:2C:5F:F9:87:59:CD:9F:08:4A:C5:EF:BA:D9:4C:18:05:69:D8:A8:03:76:60:D6:D4:26:E1:63:8E:69:36:BB:EB:98:5F:40:32:40:00:
A6:C4:9C:CA:3D:2F:82:86:DC:E9:78:8F:BE:76:5C:39:FE:01:F6:B1:29:B8:C7:6F:13:D9:94:0A:97:5D:E4:A8:A4:C2:D2:D1:07:20:3A:3D:FD:BF:99:A6:BE:FF:1F:AF:66:CB:72:61:D7:85:4A:48:78:1C:04:1C:A3:03:66:A7:1
D:B9:DB:8D:25:0D:0A:0B:DC:A8:44:82:AD:0F:CA:C7:11:E0:91:03:F6:45:C6:D1:B8:C6:91:2C:DC:63:5B:08:1E:C9:CF:4E:86:FD:7E:4D:DA:3B:9A:5A:2B:35:B8:F9:DE:15:BA:37:42:D2:8C:46:4E:89:92:68:6D:38:45:9C:F
D:7D:4A:F0:46:0A:E6:85:E6:74:F4:2E:E2:AD:DA:07:A4:D0:13:A4:7A:A7:10:3E:10:5C:3C:46:3D:BB:97:14:4C:C2:4E:D0:FE:F0:7C:0A:F3:67:AD:09:B5:FF:E1:06:32:EB:2C:A4:68:0A:F0:24:C6:EA:DE:08:F0:9B:DC:41:7
B:BF:4C:63:AD:71:18:4A:05:E4:B6:AE:2E:50:1B:56:D0:77:94:B0:1A:E0:63:F4:FC:9A:52:88:07:DB:F3:97:12:D3:EC:D7:70:3E:C3:F2:A0:8B:10:10:77:98:38:EB:88:7B:CC:90:1E:CF:EE:D4:49:6B:A3:7D:9B:1C:46:AE:C6:
A9:A7:9A:43:8A:48:2E:15:96:29:CA:3A:17:6B:2E:BF:4D:E0:AF:36:E5:07:B0:CE:43:CA:2B:42:A2:F0:4E:73:08:EC:C5:54:8B:1E:6A:CE:8E:1D:EF:DE:FC:F1:CF:5E:13:50:C8:62:69:90:CC:82:79:85:F3:31:2E:9B:5D:F7:7D
:E2:94:62:28:91:41:5F:80:1C:FA:F2:FD:72:9D:BF:E3:FE:B2:72:3E:96:20:7A:61:88:CA:10:D9:A1:CC:E0:E9:FC:8C:A2:35:C5:2B:CF:C3:E6:97:6D:11:40:B0:7C:EA:D4:1E:C3:1C:90:B3:82:FE:12:E9:4D:55:26:06:49:8D:88:
E5:71:00:5B:6C:FC:1F:84:A6:3C:21:BC:F9:1A:1B:8B:0E:C7:E3:EC:7A:04:D4:5A:12:8A:FB:FB:04:E0:29:F2:97:58:9A:15:3E:31:E4:19:D6:34:13:07:41:AD:BA:1C:86:73:9A:49:21:D9:E7:BC:AB:F2:C4:3A:0D:01:53:7D:FB
:02:17:61:29:C3:C3:08:18:8C:D2:9A:E3:53:CF:F0:8C:1A:12:43:24:C8:FE:B4:82:E2:5A:65:66:6C:20:FF:17:87:F4:FE:08:B5:96:00:C5:5F:80:78:E1:20:06:B1:0F:5D:F0:BC:4E:17:D7:C4:06:95:51:9F:DA:8E:10:11:99:D6:6F:6
D:40:CD:41:49:97:22:49:E3:3B:37:8B:4E:3A 69:71:13:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*8C:48:A3:F4:BF:0A:56:40:CA:CE:93:5D:7A:3D:26:D8:14:94:A6:CF*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*06:E6:73:D9:51:39:40:A7:D1:57:8C:36:7F:C7:ED:D0:79:DD:F7:CB*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crt* *http://ocsp.eadtrust.eu*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*22:E4:1B:48:79:FA:A2:11:61:D4:65:02:C7:FC:14:39:E5:49:0E:CC:FF:43:42:1F:6E:9C:08:61:42:70:81:96*

X509SubjectName

Subject OU:	*Legal Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust RSA 8192 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I	*jEij9L8KVkDKzpNdej0m2BSUps8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

40.9 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP*
Name	*[es]*	*Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *330884354597339267*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIE5jCCBlugAwIBAgIIBJeJkUGCOlMwCgYIKoZIzj0EAwIwgZsxQTA/BgNVBAMMOEVBRFRydXN0
IEVDQyAyNTYgUm9vdCBlQSBlGb31gUXVhbGlmaWYkIENlcnRpZmlyYXRlcyAyMDE5MS8wLQYDVQQK
DCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAW
BgNVBGEMDIZBVEVTLUI4NTYyNjI0MDAeFw0xOTA2MDYxMTIzMTJaFw0zNTA2MDIxMTIzMTJaMIGw
MT8wPQYDVQQDDDZFQURUcnVzdCBFQ0MgMjU2IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlmaWNh
dGVzIDIwMTkxLzAtBgNVBAoMJkVlcm9wZWFuIEFnZW3jeSBvZiBEaWdpdGFsIFRydXN0LCBTLUwu
MQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1NjI2MjQwMRUwEwYDVQQLDAxMZWdhbCBQ
ZXJzb24wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATWuOl18JPJcTxF2ttbytstqBRGYZB6sMGq
HRYRpEJommoO6orLRmzV9xGFl8lDjf1hfRN0wBYEigucsELa6n0uo4lCoDCCApwwgagGA1UdIASB
oDCBnTAGBgRVHSAAMIGSBg0rBgEEAYNUAgEBAYMRMIGAMCUGCCsGAQUFBwIBFhlodHRwOi8vcG9s
aWNSLmVhZHRydXN0LmV1MFcGCCsGAQUFBwICMEsMSVN1Ym9yZGlluYXRlIENlcnRpZmlyYXRlIEF1
dGhvcmI0eS4gRXVyb3BlYW4gQWdlbmNSIG9mIERpZ2l0YWwgVHU1c3QsIFMuTC4wEgYDVR0TAQH/
BAgwBgEB/wIBADAOBgNVHQ8BAA8EBAMCAYYwHQYDVR0OBBYEFNNMbDq9Nv5whyOHOu49kM/Lm/ch
MGMGA1UdEgRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRw
Oi8vY2FuaWFkdHJ1c3QuZXWGGWhtdHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwYwYDVR0RBFwwWoEO
Y2FAZWFkdHJ1c3QuZXWGFmb0dHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWb0dHA6Ly9YSS1YWR0cnVz
dC5ldYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTAfBgNVHSMEGDAWgBQBZSqExJnGge08WAR0
rySj115BDTBIBgNVHR8EQTA/MD2gO6A5hjdodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRydXN0
LXJvb3QtZWNjMjU2ZWFkcTIwMTkuY3JsMDIsGCCsGAQUFBwEBBCswaTBCBggrBgEFBQcwAoY2aHR0
cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtZWNjMjU2ZWFkcTIwMTkuY3J0MCMGCCsG
AQUFBzABhhdodHRwOi8vb2NzcC5lYWR0cnVzdC5ldTAKBggqhkjOPQQDAgNJADBGAiEAo3kjVg5x
0Nx2VI5H86QV1mB0g4miZn1xrt7SQV+8ggUCIQCOjpmf3+3shoTYYNZkUlv0aWfjV//Slps4eXGP
qoaeaQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withECDSA*

Issuer 2.5.4.97:	*VATES-B85626240*
Issuer C:	*ES*
Issuer O:	*European Agency of Digital Trust, S.L.*
Issuer CN:	*EADTrust ECC 256 Root CA For Qualified Certificates 2019*
Subject OU:	*Legal Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 256 SubCA For Qualified Certificates 2019*
Valid from:	*Thu Jun 06 13:23:12 CEST 2019*
Valid to:	*Sat Jun 02 13:23:12 CEST 2035*
Public Key:	*30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:D6:B8:E9:75:F0:93:C9:71:3C:45:DA:DB:5B:CA:DB:2D:A8:14:46:61:90:7A:B0:C1:AA:1D:16:11:A4:42:68:9A:6A:0E:EA:8A:CB:46:6C:D5:F5:C1:85:23:C9:43:8D:F7:E1:7D:13:74:C0:16:04:8A:0B:9C:B0:42:DA:EA:7D:2E*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*D3:4C:6C:3A:BD:36:FE:70:87:23:87:3A:EE:3D:90:CF:CB:9B:F7:21*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*01:67:9A:84:C4:99:C6:81:ED:3C:58:04:74:AF:24:A3:D7:5E:41:0D*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc256eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc256eadq2019.crt* *http://ocsp.eadtrust.eu*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *36:09:93:59:34:06:E5:AA:31:16:63:ED:FF:5A:34:09:A8:DD:1E:30:70:8C:9C:AB:E3:4E:FD:8E:53:92:73:3D*

X509SubjectName

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 256 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *00xsOr02/nCHI4c67j2Qz8ub9yE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_ens.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

40.10 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Certificates 2019-LP

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Certificates 2019-LP*

Name *[es]* *Certificados cualificados emitidos por ECC 384 SubCA For Qualified Certificates 2019-LP*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6351802085939901953*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFfjCCBKigAwIBAgIJWCYyWAgldgEwCgYIKoZIzj0EAwMwgZsxQTA/BgNVBAMMOEVBRFRydXN0
IEVDQyAzODQgUm9vdCBDQSBGb3lgUXVhbGlmaWYktHENlcnRpZmlYXRlcyAyMDE5MS8wLQYDVQQK
DCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMxGDAW
BgNVBGEMD1ZBVEVTLU14NTYyNjl0MDAeFw0xOTA2MDYxMTIzMTZaFw0zNTA2MDIxMTIzMTZaMIGw
MT8wPQYDVQQDDDZFQURUcnVzdCBFQ0MgMzg0IFN1YkNBIEZvciBRdWFsaWZpZWQgQ2VydGlmaWNh
dGVzIDIwMTIxLzAtBgNVBAoMJkVlcm9uZWFuIEFzZW5yeSBtZiBEaWdpdGFsIFRydXN0IUCBTLkwu
MQswCQYDVQQGEwJFUzEYMBYGA1UEYQwPVkFURVMtQjg1Nj12MjQwMRUwEwYDVQQLDAxMZWdhbCBQ
ZXJzb24wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAT16y8u3RP+c73LiVVIx3fsNqxqYmu7Xj2TxDNQ
hib7b64f+OfQB2HmmPcavFeYhdks6LmPqf+kgY30W9A43fVSfyBBqVDrNnaqJyYkfIEc4q6lNZE
TLCAZUu6mZDqWgggKgMICnDCBgAYDVR0gBIGgMIGdMAYGBFUdIAAwgZIGIDSsGAOQBg3UCAQEB
gxEwgYAwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUvVwYIKwYBBQUHAgfw
SwxJU3Vib3JkaWShdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5LiBFdXJvcGVhbiBBZ2VuY3kgb2Yg
RGlnaXRhbCBUcnVzdCwgUy5MLjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAd
BgNVHQ4EFgQUXBniqx2uD1FEpGSG4wUcdjo9YwYwYQVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWG
FmhldHA6Ly93d3cuZWFkdHJ1c3QuZXWGFWh0dHA6Ly9YS5lYWR0cnVzdC5ldYYZaHR0cDovL3Bv
bGljeS5lYWR0cnVzdC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5l
YWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1hhlodHRwOi8vcG99saWN5LmVhZHRydXN0
LmV1MB8GA1UdIwQYMBaAFHgU/e7RCWBcdadnbiZIgeTqxJIBMEgGA1UdHwRBMD8wPaA7oDmGN2h0
dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtcm9vdC1lY2MzODRlYWRxMjAxOS5jcmwwdwYI
KwYBBQUHAQEEazBpMEIGCCsGAQUFBzAChjZodHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qt
cm9vdC1lY2MzODRlYWRxMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0
LmV1MAoGCCqGSM49BAMDA2gAMGUCMDqqc9gguSlkl51ohpQPBevykIWcm1FLTwsOlr5gKccXtsVJ
6W3Z1QnCGCsYzyF8wIxAIHxWbeFz94DJlo4mv53RLthhFkLdLMnPtdeC6FFHuJFMZwTsJDFZotTF
2Dy7gLUbQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust ECC 384 Root CA For Qualified Certificates 2019*

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 384 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 13:23:16 CEST 2019*

Valid to: *Sat Jun 02 13:23:16 CEST 2035*

Public Key:


```
30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:F5:EB:2F:2E:DD:13:FE:73:BD:CB:89:55:48:C7:77:EC:36:AC:6A:62:6B:BB:5E:3D:93:C4:33:50:86:26:D3:87:AE:1F:F8:E7:D0:07:61:E6:98:F7:1
A:BC:57:98:85:D9:2C:E8:B9:8F:AA:DF:A4:81:8D:F4:5B:D0:38:DD:F5:52:7E:3C:81:06:A5:43:AC:D9:DA:A8:9C:98:91:F1:C4:7B:8A:BA:94:D6:44:4C:B0:80:65:4B:BA:8A:76:43:A9:66
```

Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu* *CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*5C:19:E2:AB:1D:B6:B8:3D:45:12:91:92:1B:8C:14:71:D8:E8:F5:F6*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://www.eadtrust.eu* *http://ca.eadtrust.eu* *http://policy.eadtrust.eu*
Authority Key Identifier	*78:14:FD:EE:D1:09:60:5C:75:A7:67:6E:26:48:81:E4:EA:C4:92:01*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc384eadq2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc384eadq2019.crt* *http://ocsp.eadtrust.eu*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*04:14:B9:54:12:A9:8B:2D:9C:8B:DD:67:16:72:19:9D:7A:9C:E5:B9:7F:69:07:38:01:AD:CB:E0:DE:D9:7B:41*

X509SubjectName

Subject OU:	*Legal Person*
Subject 2.5.4.97:	*VATES-B85626240*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 384 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I	*XBniqx22uD1FEpGSG4wUcdjo9fY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

40.11 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019*
Name	*[en]*	*Certificados cualificados emitidos por EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5049223029953283110*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHMzCCBRugAwIBAgIIRhJxmAQWRCYwDQYJKoZIhvcNAQELBQAwgYYxRjBEBgNVBAMMPUVBRFRy
dXN0IFJTQSA0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIgRVYvUFNEMiBDZXJ0IDIwMTkx
LzAtBgNVBAoMJkV1cm9wZWFulEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQG
EwJFUzAeFw0xOTA2MDYxMTM3MDJaFw0zMTA2MDMxMTM3MDJaMIGEMUQwQgYDVQQDDDtFQURUcnVz
dCBSU0EgNDA5NiBTZWJDQSBkb3IgUXVhbGlmaWYkIFdlYiBEVy9QU0QyIENlcQgMjAxOTEvMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVT
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAyl7yScyjAr2MTvJXpWgzTqonx/k3SJVY
rz70KG8Ogm57ojCUAHoMX7bJtdyAujWUY+afyGZDbVfboU/KjZ8ruimtX2eT/Al93KFjRU4Ld1Ad
r+7KiE6ilb3jCrwnsw7WnGJA+zarqExDqTsXJOJdWsVzgrE7vaWgGmx3QVa15Aen31QadKBSIPsZ
/BjRlEnLfC92vrMNjTzVE2sGQIPzfexVB4bQVvg2IGbH4xkRXSUQWz9m/wuI+rmUmMUAYLCoeBK
nNiOwwraJxzbqJuP23GM5t9xVVjRATmumKPPdgGpZQFMp7/OAbUqzSxLoCLUh5WMYULokJHTFZQi
ppX01DB/iU/IR80vHipaWdAQycgs5ez/540FmK9jFFDlHEr0k5+lSxCLvldkEGuDzmmDyVRc9tE1
Gssp53esIEj7tXXmH74032rOJz0ycGVs51KaMNCIyNHeUOwSsYvaehAmG3HWTZ+/9SBac6dlEh
8Imp2sagmLrQLKs+CIfU6N+rkmX7deOM6hsdIDnHfsXBWhB8mRgBj/WuX4dnkjs67HK6MKb/FGoM
CyihISNN9PMFJQOMGIy1Lvw7U1LdlxcJfwqmT4rzUiXNL3DcHa9Aj+Qd7SEGw0Rjr0oWustEdLPq
fZXVsvzJDLcpfhTnzc29OtvPaMuppdLXkVAGuHoTmvkCAwEAAaOCAaMwggGIMEsGA1UdIAREMEIw
BgYFVR0gADA4Bg0rBgEEAYNfAgEBAYMRMCcwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb2xpY3kuZWFk
dH1c3QuZXUwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFITO
82uqplcwJ/fDEpkg5eCbWh5EMB8GA1UdIwQYMBaAFLQcKNTqgmAPEAR0y3eUaUwRh+JEME4GA1Ud
HwRHMEUwQ6BBoD+GPWh0dHA6Ly9jcmwuZWFkdH1c3QuZXUvZWFkdH1c3Qtcm9vdC1yc2E0MDk2
ZWFkZXZwc2QyMjAxOS5jcmwwfQYIKwYBBQUHAQEEcTBvMEgGCCsGAQUFBzAChjxodHRwOi8vY2Eu
ZWFkdH1c3QuZXUvZWFkdH1c3Qtcm9vdC1yc2E0MDk2ZWFkZXZwc2QyMjAxOS5jcmQwIwYIKwYB
BQUHMAGGF2hodHA6Ly9vY3NwLmVhZHRydXN0LmV1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEF
BQcDAjANBgkqhkiG9w0BAQsFAAOCAgEAnVdxWWcf0MEm7lhVxgNgaiGr5lsxPnZvme9gc1XL8Wl4
8Nbcoq57ZHwHqWwHlVpUDz1gxPC963jfjgZgr/6ows7S5IQ9fOZqPsoL9axi9LOk9F74s7/JRyR
gqnvkmW2u1b4WLB92KJHXgbCzzJSS7a+uTqqaBerU2lMNM0fID3FD1QbXWvb2pK5ukdauuQKnujA
JRLLiUsorhUdGMM/0uUjokzywAizc051DGzIUdrbqfVOp1yik2zdS3XmcG0mY+/P+0lLiKFfTv10
jyTnyxIt5zL/b9uliyjq3Uy2ZJ6WPdYuFhlyVCjEW8Nns3Gnc4KgHUwtM5DKS39q4U/MzuY2E5p
9E5gRT5ZWxekrc2MCGSoQcjbpKozDlAFx7V6FZdN3D8tJA0C22MLblaSNg0Wxh1HnN3/tP93Jogw
KNuHQcYAzIvXK5Pl4lCokl8QuQNbGZT3uJLMlFiEhNdxjBU/LahjE2yhtL/t+1ZUgHYjVEk03CQv
35zTPDcWZSUj/GcxOURoAvQcloTPCF/ydbfgD4vVaoESERX0vvtjbZw2TW4HHvsx6uGY+INVSsU/T
HjoWbuwsx/x/jmdHoVi1QrQbWfzIpyOvhcoyxuFNDeBd8RB0PXv0O3dWTMzScQWPga7HZmo24ZHQ
ivDguM8/3NuSF/lKI2p/Eh7g2JPEGSI=

-----END CERTIFICATE-----
```

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 4096 Root CA For Qualified Web EV/PSD2 Cert 2019*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019*

Valid from: *Thu Jun 06 13:37:02 CEST 2019*

Valid to: *Tue Jun 03 13:37:02 CEST 2031*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CA:5E:F2:49:EC:A3:02:BD:8C:4E:F2:57:A5:68:33:4E:AA:27:C7:F9:37:48:95:58:AF:3E:F4:28:6F:0E:82:6E:7B:A2:30:94:00:7A:0C:5F:B6:C9:B5:DC:80:BA:35:94:63:E6:9F:C8:66:43:6D:57:DB:A1:4F:CA:8D:9F:2B:BA:29:AD:5F:67:13:FC:02:3D:DC:A1:63:45:4E:0B:77:50:1D:AF:EE:CA:88:4E:A2:8A:1D:E3:0A:7C:27:B3:0E:D6:9C:62:40:FB:36:AB:A8:4C:43:A9:3B:17:24:E0:DD:5A:C5:73:82:B1:3B:BD:A5:AA:1A:6C:77:41:56:B5:E4:07:A7:DF:54:1A:74:A0:52:94:F8:99:FC:18:D1:94:49:D4:0B:DD:AF:AC:C3:63:4F:35:44:DA:C1:90:20:F7:7A:C5:50:78:6D:05:6F:81:92:06:6C:7E:31:91:15:D2:51:05:B3:F6:6F:F0:B8:8F:AB:9A:25:26:C4:C5:00:63:F2:C2:A1:E0:4A:9C:D8:8E:C3:0A:DA:27:1C:DB:A8:9B:8F:DB:71:8C:E6:2F:71:55:58:D1:01:39:AE:98:A3:CF:76:01:A9:65:01:4C:A7:BF:CE:02:15:2A:CD:2C:4B:A0:22:D4:87:95:8C:61:42:E8:90:91:D3:15:94:22:A6:95:F4:D4:30:7F:89:4F:E5:47:CD:2F:1E:2A:5A:59:D0:10:C9:C8:2C:E5:EC:FF:E7:8D:05:98:AF:62:14:50:C8:1C:4A:F4:93:9F:A5:4B:10:8B:BE:57:64:10:6B:83:CE:69:83:C9:54:5C:F6:D1:35:1A:2B:2C:A7:9D:DE:B1:F1:23:EE:D5:D7:98:7E:F8:D3:7D:AB:38:9C:F4:C9:C1:95:B3:9D:4A:68:C3:42:97:23:47:79:43:B0:4A:C6:2F:69:E8:40:98:6D:DF:5A:5E:D9:FB:FF:52:05:A7:3A:76:51:21:F0:89:A2:A7:6B:1A:82:62:E2:40:B2:AC:F8:27:E5:53:A3:7E:AE:49:97:ED:D7:8E:33:A8:6C:74:90:E7:1E:C5:C1:FD:68:41:9B:C8:01:8E:55:AE:5F:87:67:92:3B:3A:EC:72:BA:30:A8:7F:14:6A:0C:0B:28:A1:21:23:4D:F4:F3:05:25:03:8C:18:8C:B5:2E:FC:3B:53:52:DD:97:17:09:7F:0A:A6:4F:8A:F3:52:25:CD:2F:70:DC:1D:AF:40:8F:E4:1D:ED:21:06:C3:44:63:CF:4A:16:BA:CB:44:74:B3:EA:7D:95:D5:B2:FC:C9:0C:B7:29:7E:14:E7:CD:CD:BD:3A:DB:CF:68:CB:A9:A5:D2:D7:91:50:06:B8:7A:13:9A:F9:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: http://policy.eadtrust.eu

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *84:CE:F3:6B:AA:A6:57:30:27:F7:C3:12:99:20:E5:E0:9B:5A:1E:44*

Authority Key Identifier *B4:1E:28:D4:EA:AA:60:0F:10:04:74:CB:77:94:69:4C:11:87:E2:44*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa4096eadevpsd22019.crl*

Authority Info Access

http://ca.eadtrust.eu/eadtrust-root-rsa4096eadevpsd22019.crt

http://ocsp.eadtrust.eu

Extended Key Usage *id_kp_serverAuth*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *00:9D:BA:D6:86:CE:CD:81:D1:3A:CA:C4:F6:73:DC:BA:5E:EB:78:9E:63:17:3C:DE:13:6C:B2:88:0C:1D:CE:79*

X509SubjectName

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019*

X509SKI

X509 SK I *hM7za6qmVzAn98MSmSDl4JtaHkQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI [es] *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.12 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019*

Name [es] *Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number:

8543911274838307584

X509 Certificate

-----BEGIN CERTIFICATE-----

MIILMzCCBxugAwIBAgIIdpISCXExMwAwDQYJKoZIhvcNAQENBQAwgYYxRjBEBgNVBAMMPUVBRFRy
dXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIgRVYvUFNEMiBDZXJ0IDIwMTkx
LzAtBgNVBAoMJkV1cm9wZWFuIFFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQG
EwJFUzAeFw0xOTA2MDYxMTQ5MTBaFw0zMTA2MDMxMTQ5MTBaMIGEMUQwQgYDVQQDDDtFQURUcnVz
dCBSU0gzODI5MzBTdWJDQSBhZGJlaWVkIFdlYiBlYW9QU0QyIEXlcnQgMjAxOTEvMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmNSIG9mIERpZ2l0YWwgYHJ1c3QsIFMuTC4xC2A/BgNVBAYTAkVT
MIIEIjANBgkqhkiG9w0BAQEFAAOCBA8AMIIECgKCBAEAsSLKuBGGPqZpFmyeIJdi4SKUoXxS8ikb
xnLJsd5SbVdkSFLAbQWuhqrgXCuGCgoWd1mSN+6ERdZCXJ5TtlICpVc1H0fvuFQSklPI+//NjS0
IBw+iZk/5iUzX6+gnE1fhm2UDhND90ZK2S31MI0B27s/ZXBO3LpjbjUE/F0tcPiYec4G23odTrq
SczZTjnJAnw4ZSB4To4G6bFtFQbIKCAicM50KsbWN9pfsI4mhIEepTnVd8umSOkEPNecOuf6izdK
ncOBPkkzkJorgLwP/C8YTAEyXSPdI4KCz8pQQSmIfGJ7b4DSs/DpR1dKTOXko5Sx5ouz3H5TY4x
6/LXxJBzKTDcy4Dpaoon3OaDulAUHO0xH872s5FEZu/QDoRLhQ6fQCdOQKKHIIe9V6/RXyNrdBDDB
+zL74aw/7aydQRzv8R5v9RobMBjDAQujnZH2P8/dz3bThbhOrTWzMBKQ0uOWoVr7Ghcwg2thxVqEG
xYv+tD+3RQpvvNar2nm/sZKm3OnBkqw3a7YTqj4+rqj+NZQHNpbSnCTCb5yqBP5fZOqs4iL+zsO
8lyClBUbll7w1yy/BwiPR90g2ddlVmmLXcS6FA1/nzVgbDzGQsyrjHOjYXBLf3PKNRx7GiBYpGL
AhN/EQLsvksÚNTMZWqeor46S6u/maKH95yNPENQc/2ycBGvIlAQ9yq5D2gNOM/AVBQ/u85yYNa9R
XsG1OcgdusnNm7lvut2GjbLwaAChFmG+W+AmteQtQdAsEoZsNLHTzZ/W0F9fgtlNOqXXm3llZkpU
LmQqcSXYpr/cpz+/NhL91JYkTT+1NxDSKovEidjRfdbVZgu2uGMvdssPlfCXLwnaLF8H4ZcKCpDG
E59WwuGPD2XabhCx5JcbG+LsXNUiaI8KStqAVqp7cporbQxoqPzxvXDlNrvWojuAJhp+Ad0WVGqP
uQ9+FkwANs9NrjavMLd6z/+7ycXPUK6ASLLCRh9En5WGi9IpgyZNonTYDX/s/S1ZlJhrcjo2etzoc
MhedUaStQhnoXL NxNwMRaVqKzfaivn1BlVpRhHLYz5hU0geudkmzPhodtq9vbbHzyEJACSpbr+jS4
wOlLzhuSMRYBEGa016kmVQnzbMLQwV/JFA/X9MKRLNzkSOnfoSx2N2N9V0
LOXzQsmIywvvqEDKv+nypoEn/xV2pVXx8yOjqmzIrIzOVYvYd/ex0gJj8O3vhxcmQWF+/4ENNB
OaU3PsbXC7KiWVxq/qulX3jv6KqCrjCL/+bDt9xcmZzx7byreMyITBMOAAoPo/k7UhmvQKDbezk
PbgnU/k0uPNYi2tc5ggMTVdZc7rzJVDnzEAgyTH42QIDAQABo4IBozCCAZ8wSwYDVR0gBEQwQjAG
BgRVHSAAMDgGDSsGAQQBg5HtCAGEBgxEwIsAIBgarBgEFBQcCARYZaHR0cDovL3BvbGljcs51YWR0
cnVzdC5ldTASBgNVHRMBAf8ECDAGAQH/AgEAMAkGA1UdDwEBwQEAwIBhjAdBgNVHQ4EFgQUDmLL
aHy9Yxsoi1Qhrg+NpHEnll4wHwYDVR0jBBgwFoAUumoOmCc2HKo0TdtV992wc0nzXfcwTgYDVR0f
BEcwRTBDoEGgP4Y9aHR0cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTgxOTJl
YWRldnBzZDJyMDE5LmNybDB9BggrBgEFBQcBAQRxMG8wSAYIKwYBBQUHMAKGPGhhdHAsLy9jYS5l
YWR0cnVzdC5ldS9lYWR0bnVzdC1yb290LXJzYTgxOTJlYWRldnBzZDJyMDE5LmNyodDAjBggrBgEF
BQcwAYYXaHR0cDovL29jc3AuZWFkdHJ1c3QuZXUwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMA0GCSqGSIb3DQEBDQUAA4IEAQDGczJzPVt6JVluaxQLSGg9WHHd8eza05FtO3h9WO6jZJ0F
QUn79hze619uap5Cj6NhLiRXL2HbN2F7HgsU591Ccedl1vMsZnCgP6+itMtfxVSBCSR578SJfjwEr
czD1P6IyID7r68oI3mSn0YdhkVWXE0Ia+uvsNl0HI4VjGho9RuSTdbl4scFiIdTCYY9F+kouF2G
e6SUn1Camcnqvm1KCR88dBszfCMPtKiDoLI49B/Plb31f06a6aKk/WZg77bGzi16FOVKHdKkoDOwz
v74HTp99JJM/kJVbWkZj1nEA3yX8KK96+bx0YpGuywuEMTKazfiujwWXViam5DDzWB921QeBO0Kwa3
ev8LuHGLbSNyriRhzSvx/Bj3i9r4/CoqTTyRPfA8EkaIHjWATXrtqeSI2KrpP6V7m/2Xe66HFiND
dRYf6Uqg59+L0rpjFuFrNvG9Wmnk2MfMXY01l5NyYg3ns5LXZmMCOd+3yZfvsqGtDYw5JV8
ZfW7i0CbdD+Vfuipvl7yXkP+0rmrPVc3RKtABzkFl1zYYz4AkIuWfAZ1TSC+e3/zTy01tN9LkKFq
2ioOky3GLReTjUmVjMRf/quUsHacbqQZmHTwlwjK073vk7kEMlrB+awFGhBVG8vUKfooAAoSr9c2
7ZkONJcjSjRFTMa1/2l/oAXxSebF7dlLguLA31aiMn0VqMWUnBCYcDgA89EXQ0vGyoWFSzoU5JNO
y4gWvwwpAvIMo7rAab37sh6OwkrEnRGBLD3m+ezFCuNRdIEnSdIt/PZKnXLXvbMKlILFU1a689
HWwVCYQhXkO3WwJBvpNcsCUQKuZQtYGuTVhoj+BtXPzKI9H2ZKyWqb1SvxSatjEW1+FQ9DCi3jG
LAzcQDVCNxs+17Tx0Ex3nVGg2nsKU61dlbKdPh9hJBkgWsid5mytHiYuwRbO1Dd8ZHRGOJL/cQwC
0WfpB/VQtN4RJiau0GJjuKAUdJcV4y2y1XlsE6GZUiRw9kaAcMbmZtTcLwdDCTjzNKSUX6WtYTst
Pbxph6y2Ch3t59VG8Umw/O90kwQ8JVnG4ooFsevgqmmgq1Ov59X6KV3sqwAcKWU4MUBvsIiRzOQ
5IhL5FNkqx8scxrnyjXTssvH66GPONzGKZQGYIAAEVCzMoYncnXykM13G525eVoQs715ckOPbnkfl
e5JWVDn7udyaZC1SRGZaJKonLSFnVC7oEheBCqGe9eL6y4GalcTNHlhT1dXsFGVhmjc6EAmZ96fB
4L6bFihBgIfu1MUnwuARK32EDcSAcvS7Ilc/mZrSm+GXYw0S8nVbet1gNql98wWM/PJnEVmQrO2
JVQ2BsR/j9eiHFc6qKmC1/SZK9IP

-----END CERTIFICATE-----

Signature algorithm:

SHA512withRSA

Issuer C:

ES

Issuer O:

European Agency of Digital Trust, S.L.

Issuer CN:

EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019

Subject C:

ES

Subject O:

European Agency of Digital Trust, S.L.

Subject CN:

EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019

Valid from:

Thu Jun 06 13:49:10 CEST 2019

Valid to:

Tue Jun 03 13:49:10 CEST 2031

Public Key:

30:82:04:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:B1:22:CA:B8:11:86:3E:A6:69:16:6C:9E:20:97:62:E3:92:94:A1:7C:52:F2:29:1B:C6:72:C9:B1:DE:52:85:57:64:48:52:
C0:85:05:AE:86:AA:E0:5C:2B:86:0A:0A:16:77:59:92:37:EE:84:45:D6:42:5C:9E:53:B4:89:42:A5:57:07:1F:47:EF:B6:E1:50:4A:49:4F:53:EF:FF:36:34:B4:20:1C:3E:89:99:3F:E6:25:33:5F:AF:A0:A4:4D:5F:86:6D:94:0E:13:4
3:F4:96:4A:D9:2D:F5:30:8D:01:DB:BB:3F:65:70:4E:DC:BA:63:6E:35:04:FC:5D:2D:70:F8:98:79:CE:22:1B:6D:E8:75:3A:E4:49:CC:D9:12:92:40:9F:0E:36:48:1E:13:A3:81:9F:A0:5B:45:42:12:11:08:08:9E:33:93:8A:2A:C6:
D6:37:DA:5F:B0:8E:26:84:81:1E:A5:39:D5:77:CB:A6:48:E9:04:3C:D7:9C:3A:E7:FA:8B:39:A9:2B:80:BC:0F:FC:2F:18:4C:01:32:5D:23:DD:23:82:82:CF:CA:50:41:29:9F:94:67:C9:ED:BE:03:4A:
CF:C3:A5:1D:5D:29:33:97:92:8E:52:C7:9A:2E:CF:71:F9:4D:8E:31:EB:F2:D7:C4:90:73:29:30:DC:CB:80:E9:6A:8A:27:DC:E6:83:BA:50:14:1C:ED:31:1F:CE:F6:B3:91:44:66:EF:D0:0E:84:4B:85:0E:9F:40:27:4E:40:A2:87:2
0:4F:55:EB:F4:57:C8:DA:DD:04:30:C1:FB:32:FB:E1:AC:3B:6B:27:50:47:3B:FC:47:9B:FD:46:86:CC:06:30:C0:42:E8:E7:64:7D:8F:F3:F7:73:DD:B4:E1:F1:B3:AB:4D:6C:CC:04:A4:34:B8:E5:A8:56:BE:C6:85:CC:20:66:D8:
71:56:A1:06:C5:8B:FE:AC:3F:B7:44:EA:6F:BC:D6:AB:DA:79:BF:FE:C6:4A:9B:93:A7:D2:4A:B0:DD:AE:D8:4E:A8:F8:FA:BA:A3:F8:DD:90:1C:DA:61:4A:70:93:09:BE:72:A8:13:F9:7D:93:9A:E2:DD:4B:FB:3B:0E:F2:5C
:82:97:C5:1B:94:8E:F0:D7:2C:BF:07:08:8F:47:DD:20:D9:D7:48:56:69:8B:5D:E4:BA:14:02:3F:9F:35:60:6C:3C:C6:42:CC:AB:8D:F1:CE:8D:85:C1:2D:FD:CF:28:D4:71:EC:68:81:62:91:8B:02:13:7F:11:02:EC:BE:4B:14:35:
33:19:5A:A7:A8:AF:BE:92:EA:EF:E6:68:A1:FD:E7:23:4F:10:D4:1C:FF:6C:9C:04:6B:E5:20:04:3D:CA:AE:43:DA:03:4E:33:F0:15:05:0F:EE:F3:9C:98:35:AF:51:5E:C1:B5:39:C8:1D:BA:C9:CD:9B:B9:6F:BA:DD:86:8E:12:
F0:68:00:A1:16:61:BE:5B:E0:26:B5:E4:2D:41:D0:2C:12:86:6C:34:B1:D3:CD:98:D6:D0:5F:5F:82:D9:4D:42:A5:D7:9B:79:48:66:4A:54:2E:64:2A:7B:95:D8:A6:BF:DC:8A:9D:BE:36:12:FD:D4:96:24:21:3F:B5:37:10:D2:2A:
8B:C4:89:D8:D1:7D:D6:D5:66:0B:B6:B8:63:2F:76:CB:0F:96:51:97:2F:09:DA:2C:FD:F4:E1:97:0A:0A:90:C6:13:9F:56:5A:E1:8F:0F:65:DA:6E:10:B1:E4:97:1B:1B:E2:EC:5C:D5:22:69:FF:0A:4A:DA:80:56:AA:7B:72:9A:2
B:6D:0C:68:AB:FC:F1:BD:70:E5:36:BB:D6:A2:3B:80:26:1A:7E:01:DD:16:54:6A:8F:B9:0F:7E:16:4C:00:36:CF:4D:AE:36:AF:30:B7:7A:CF:FF:BB:C9:C5:CF:50:AE:80:48:B2:C2:46:1F:44:9F:95:86:8B:DD:29:82:F6:4D:A2:
74:D8:0D:7F:EC:FD:2D:59:D6:1A:DC:8E:8D:9E:B7:3A:1C:32:17:9D:51:A4:AD:42:19:E8:5C:B3:71:37:03:11:69:5A:8A:CF:46:AF:9F:50:65:56:94:61:1C:B6:33:E6:15:34:81:EB:9D:92:6C:CF:B6:87:6D:AB:DB:DB:6C:7C:F
2:10:90:02:4A:96:EB:FA:34:B8:C1:07:CB:CE:1C:12:31:15:5F:10:66:B4:D7:A9:26:57:6A:9B:03:6E:88:77:30:19:06:84:1E:8B:B7:D4:9B:5D:44:A4:C2:D0:C1:5F:C9:14:0F:D7:F4:C2:91:2C:DA:E4:B0:EB:E7:12:C5:F6:37:D5:
74:2C:E5:F3:42:C9:88:CB:0B:FF:AE:A1:03:2A:FF:A7:CA:9A:04:9F:FC:55:DA:95:57:C7:CC:8E:8E:3A:A6:CC:8A:E5:CC:E5:58:BD:87:7F:7B:1D:20:26:3F:0E:DE:F6:F1:72:64:16:17:EF:F8:10:D3:41:39:A5:37:3E:C6:D7:0
B:B2:A2:59:5C:6A:FE:AB:A5:78:EF:E8:AA:82:AE:30:8B:FF:E6:C3:7F:DC:5C:99:9C:F1:ED:BC:AB:78:CC:9F:25:30:4C:38:00:28:3E:8F:E4:ED:48:66:BD:02:83:6D:EC:E4:3D:B8:27:52:4D:2E:3C:D6:22:DA:D7:B9:82:0
3:13:55:D6:5C:EE:BA:F3:25:50:E7:CC:40:20:C9:31:F8:D9:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: http://policy.eadtrust.eu

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

0E:62:CB:68:7C:BD:63:1B:28:8B:54:21:AE:0F:8D:A4:71:27:22:5E

Authority Key Identifier	*BA:6A:0E:98:27:36:1C:AA:34:4D:DB:55:F7:DD:B0:73:49:F3:5D:F7*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22019.crt* *http://ocsp.eadtrust.eu*
Extended Key Usage	*id_kp_serverAuth*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*51:4A:80:6A:46:D7:B7:97:25:B9:2C:EA:06:85:54:15:D9:24:E7:6D:C5:D5:1E:4E:D5:CA:39:55:CB:6E:C8:5D*

X509SubjectName

Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019*

X509SKI

X509 SK I	*DmLLaHy9Yxsoi1Qhrg+NpHEnIl4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.13 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

Name *[es]* *Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3612576674077687876*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDpDCCA0mgAwIBAgIIMiJzWEZDQEQwCgYIKoZIzj0EAwIwgYUxRTBDBgNVBAMMPEVBRFRydXN0
IEVEQyAyNTYgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBFV19QU0QyIENlcnQgMjAxOTevMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xC2AJBgNVBAYTAkVT
MB4XDTE5MDYwNjExNDkyNFoXDTMxMDYwMzExNDkyNFowgYMxQzBBBgNVBAMMOkVBRFRydXN0IEVD
QyAyNTYgU3VC0lIgRm9yIFF1YWxpZmllZCBXZWIgRVYsUFNEMiBDZXJ0IDIwMTkxLzAtBgNVBAoM
JkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzBZMBMG
ByqGSM49AgEGCCqGSM49AwEHA0IABCoD0KVinA0yE58PK9ttDhp24ao177XI+uEN1ck+PYZhgDZZ
cD5TkjDrGlC2UchXlw24U1/plMMbZNVVf4KhBzWjggGhMIIBnTBLBgNVHSAERDBCMAYGBFUdIAAw
OAYNKwYBBAGDdQIBAQGDET AnMCUGCCsGAQUFBwIBFhlodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1
MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBQJdlR5ZrQBosRSS
VUEGb7NmMDkgczAfBgNVHSMEGDAWgBTTd81a2qOTXItKTGXSmgwB1Zk/EzBNBgNVHR8ERjBEMEKg
QKA+hjxodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtZWNjMjU2ZWFkZXZwc2Qy
MjAxOS5jcmwwIAYIKwYBBQUHAQEEcDBuMEcGCCsGAQUFBzAChjtodHRwOi8vY2EuZWFkdHJ1c3Qu
ZXUvZWFkdHJ1c3Qtcm9ydC1lY2MyNTZlYWRtbnBzZDIyMDE5LmNvdDAjBggrBgEFBQcwAYYXaHR0
cDovL29jc3AuZWFkdHJ1c3QuZXUwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMAoGCCqG
SM49BAMCA0kAMEYCIQC26I5acV5Y/bM0ZDI6w43s7lbd86MlqAvrX8yciDv+6AIhAPPNHzRucILM
LzkpHGqvNF1pa1AzzB3ryo3TE5Ai2Lyy

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withECDSA*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

Valid from: *Thu Jun 06 13:49:24 CEST 2019*

Valid to: *Tue Jun 03 13:49:24 CEST 2031*

Public Key:


```
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:2A:03:D0:A5:62:9C:0D:32:13:9F:0F:2B:D8:ED:0E:1A:76:E1:AA:35:EF:B5:C8:FA:E1:0D:D5:E9:3E:3D:86:61:80:36:59:78:3E:53:92:3
0:EB:18:80:B6:51:C8:57:87:0D:B8:53:5F:E9:94:C3:1B:64:D5:55:7F:82:A1:07:35
```

Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*09:75:1E:59:AD:00:68:B1:14:92:55:41:06:6F:B3:66:30:39:20:73*
Authority Key Identifier	*D3:77:CD:5A:DA:A3:93:5C:8B:4A:4C:65:D2:9A:0C:01:D5:99:3F:13*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc256eadevpsd22019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc256eadevpsd22019.crt* *http://ocsp.eadtrust.eu*
Extended Key Usage	*id_kp_serverAuth*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B7:69:11:A3:35:2D:1A:27:B3:C3:55:F0:49:CF:6F:BF:C5:E3:E4:97:5B:FD:BD:BC:1F:A0:41:32:7F:C7:6D:7C*

X509SubjectName

Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

X509SKI

X509 SK I	*CXUeWa0AaLEUklVBBm+zZjA5IHM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.13.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.14 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

Name *[es]* *Certificados cualificados emitidos por EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *311084161010393909*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIID3zCCA2agAwIBAgIIBFExZXBGYzUwCgYIKoZIzj0EAwMwgYUxRTBDBgNVBAMMPEVBRFRydXN0
IEVDQyAzODQgUm9vdCBDQSBGb3IgUXVhbGlmaWVkIFdlYiBFVi9QU0QyIENlcnQgMjAxOTevMC0G
A1UECgwmRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVT
MB4XDTE5MDYwNjExNDkyNloXDTMxMDYwMzExNDkyNlowgYMxQzBBBgNVBAMMOkVBKFRydXN0IEVD
QyAzODQgU3Vi0IEgRm9yIFF1YWxpZmllZCBXZWIgRVYsUFNiMiBDZXJ0IDIwMTkxLzAtBgNVBAoM
JkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzB2MBAG
ByqGSM49AgEGBSuBBAAiA2IABA/E/MZip8kQYbCd6ULS02ZFHo3mMWXNPX2TgKPzHlkRvEO6W25X
PT7kHgaJQkBXbN3runWSrd0jO+VOTpXZRizLMrwpwL4fHqOCzZNiryxd0BsSscTDAwsdSlN+c3a
patOCAaEwggGdMEsGA1UdIAREMEIwBgYFVR0gADA4Mg0GBgEEAYNJAgEBAYMRMCcwJQYJKwYBBQUH
AgEWGWh0dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8B
Af8EBAMCAYYwHQYDVR0OBBYEFHG7WKA8L1SHXQt7UUg4q2DXqqnjMB8GA1UdIwQYMBaAFOrpUOSz
k0k/BQQ1pfBHVxF+XhEZME0GA1UdHwRGMEQwQqBAoD6GPGh0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUv
ZWFkdHJ1c3Qtcm9vdCI1Y2MzODRlYWRidnBzZDIyMDE5LmNybDB8BggrBgEFBQcBAQRwMG4wRwYI
KwYBBQUHMAKGO2h0dHA6Ly9jYS5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LWVjYzM4NGVhZGV2
cHNkMjIwMTkuY3J0MCMGCCsGAQUFBzABhhdodHRwOi8vb2Nzcc5lYWR0cnVzdC5ldTAdBgNVHSUE
FjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwCgYIKoZIzj0EAwMDZwAwZAIwGtzHs7pl00elA9QaPgjG
bZrH2AUuzS+0Ip0OpPpAqsavD6sIEBAIDV+QIpD0Ga+AjABhvTQpMrL7vJgjaGimVIgisJqhgNZ
82WDmERYQ9dR8ETvlzVWkCLboXvF0tszIl4=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2019*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

Valid from:	*Thu Jun 06 13:49:26 CEST 2019*
Valid to:	*Tue Jun 03 13:49:26 CEST 2031*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:0F:C4:FC:C6:62:A7:C9:10:61:B0:9D:E9:42:D2:D3:66:45:1E:8D:E6:31:65:CD:3D:7D:93:80:A3:F3:1E:59:11:BC:43:BA:5B:6E:57:3D:3E:E4:1E:06:89:42:40:57:6C:DD:EB:BA:75:92:AD:DD:23:3B:E5:4E:4E:95:D9:46:2C:CB:32:BC:29:C0:BE:1F:1E:A3:BF:0B:36:4D:8A:BC:B1:77:40:6C:4A:C7:13:0C:0C:2C:75:29:4D:F9:CD:DA:A5*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*71:BB:58:A0:3C:2F:54:87:5D:0B:7B:51:48:38:AB:60:D7:AA:A9:E3*
Authority Key Identifier	*EA:E9:50:E4:B3:93:49:3F:05:04:35:A5:F0:47:57:11:7E:5E:11:19*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc384eadevpsd22019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc384eadevpsd22019.crt* *http://ocsp.eadtrust.eu*
Extended Key Usage	*id_kp_serverAuth*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C8:79:2B:47:35:5F:A3:D1:52:AA:5E:86:F3:7C:27:65:0B:E1:E0:51:37:BD:36:E8:77:8A:CF:27:0B:B1:8B:54*

X509SubjectName

Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

X509SKI

X509 SK I	*cbtYoDwvVIddC3tRSDirYNeqqeM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.14.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.15 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019*
Name	*[es]*	*Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1258060407115912249*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDnDCCA0GgAwIBAgIIEXWHRlggIDkwCgYIKoZIzj0EAwIwgYMxQzBBBgNVBAMMOkVBRFRydXN0
IEVDQyAyNTYgUm9vdCBDQSBGb3IgUXVlbGlmaWVkIFdlYiBEVi9PViBDZXJ0IDIwMTkxLzAtBgNV
BAoMJkV1cm9wZWFuIEFnZW5jeSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAc
Fw0xOTA2MDYxMTM1NTJaFw0zMTA2MDMxMTM1NTJaMIGBMUEwPwYDVQQDDDhFQURUcnVzdCBFQ0Mg
MjU2IFN1YkNhIEZxciBRdWFsaWZpZWQgY2VuIERWL09WIENlcnQgMjAxOTEvMC0GA1UECgwmRXVy
b3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMFkwEwYHKoZI
zj0CAQYIKoZIzj0DAQcDQgAEQmqP2YJy3ACaPj9Mu1FcH2UTDK5U6zrXoPr/+1cA0VayagC9JFB0
2g/xej3X9tv55c9V8iU/iwSLA70VoFbNMjaOCAZ0wggGZMEsGA1UdIAREMEIwBgYEVR0gADA4Bg0r
BgEEAYN1AgEBAYMRMCcwJQYIKwYBBQUHAgEWGWh0dHAsL y9wb2cpY3kuZWFkdH1c3QuZX1/wEgYD
VR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFOCbgvBL7ZoiOqfi6Av
/hWIrJVkMB8GA1UdIwQYMBaAFLwrx1vjatp90ahGrUfe40XAw/2yMEsGA1UdHwREMEIwQKA+oDyG
Omh0dHA6Ly9jcmwuZWFkdH1c3QuZX1/vZWFkdH1c3Qtcm9vdC1lY2MyNTZlYWRkdm92MjAxOSSj
cmwwegYIKwYBBQUHAQEEbjBsMEUGCCsGAQUFBzAChjloaHRwOi8vY2EuZWFkdH1c3QuZX1/vZWFk
dH1c3Qtcm9vdC1lY2MyNTZlYWRkdm92MjAxOS5jcnQwJwYIKwYBBQUHMAGGF2htdHAsLy9vY2Nw
LmVhZHRydXN0LmV1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAKBggqhkjOPQQDAgNJ
ADBGAiEA+xsp1y3d0b/kLk+9bqHxlTXznZQSSjYmiBQCpv8kabsCTQCaLjx5plNhyGTWMRoaSNw0
fSAkivbPUopn55pcCu8Cjg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withECDSA*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019*

Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019*
Valid from:	*Thu Jun 06 13:35:52 CEST 2019*
Valid to:	*Tue Jun 03 13:35:52 CEST 2031*
Public Key:	*30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:42:6A:8F:D9:82:72:24:00:9A:3E:3F:4C:BB:51:5E:1F:65:13:0C:AE:54:EB:3A:D7:A0:FA:FF:FB:57:00:D1:56:B2:6A:00:BD:24:50:74:DA:0F:F1:7A:3D:D7:F6:DB:F9:E5:CF:55:F2:25:1F:C3:92:C0:EF:45:68:15:B3:4C:8D*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*E0:9B:82:F0:4B:7F:B6:68:88:EA:9F:B7:A0:2F:FE:15:A5:AC:95:64*
Authority Key Identifier	*BC:2B:C7:5B:E3:6A:DA:7D:D1:A8:46:AD:47:DE:E3:45:C0:C3:FD:B2*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crt* *http://ocsp.eadtrust.eu*
Extended Key Usage	*id_kp_serverAuth*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*0E:1F:3A:20:04:0E:D5:B2:72:DC:C9:39:E7:B8:D5:B0:F4:BE:D7:64:C9:5C:E1:6C:B0:A4:7C:A4:56:0A:36:95*

X509SubjectName

Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019*

X509SKI

X509 SK I	*4JuC8Et/tmiI6p+3oC/+FaWslWQ=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*

	[es]	*undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.16 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019*
Name	*[es]*	*Certificados cualificados emitidos por EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5773670184699650920*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIDIzCCA16gAwIBAgIIUCAycVlJY2gwCgYIKoZIzj0EAwMwgYMxQzBBBgNVBAMMOkVBRFRydXN0
IEVDQyAzODQgUm9vdCBDQSBGb3lgUXVhbGlmaWVkIFdlYiBEVi9PViBDZXJ0IDIwMTkxLzAtBgNV
BAoMJkV1cm9wZWFuIEFnZW5jcSBvZiBEaWdpdGFsIFRydXN0LCBTLkwuMQswCQYDVQQGEwJFUzAc
Fw0xOTA2MDYxMTM1NTVaFw0zMTA2MDMxMTM1NTVaMIGBMUEwPwYDVQQDDDbFQURUcnVzdCBFQ0Mg
Mzg0IFN1YkNBIEZvciBRdWFsaWZpZWQgY2VlIERWL09WIENlcnQgMjAxOTEvMC0GA1UECgwmRXVy
b3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4xCzAJBgNVBAYTAkVTMHYwEAYHKoZI
zj0CAQYFK4EEACIDYgAE6o4xOzPzH2Hf9WK476vEYj6nkC3GiYomL9YSRu0gzdi2oSlm8eZcGEuD
7pe0Gd3Y8JL7A1vgRzlUa+TUuftPjB4MfWLz79VcHZCRxtFZrxRuesb4HN61haPgkk7sFSUxo4IB
n1CCAZkwSwYDVR0gBEQwQjAGBgRVHSAAMDgGDSsGAQQBg3UCAQEBgxEwIzAIBggrBgEFBQcCARYZ
aHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQE
AwIBhjAdBgNVHQ4EFgQUZj/V6yyw0c/kc+YXwGjFc+pv9kowHwYDVR0jBBgwFoAUHJTYEpRJf9et
Q3G7LrK6M9L A9EYwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0
cnVzdC1yb290LWVjYzM4NGVhZGR2b3YyMDE5LmNybDBbBggrBgEFBQcBAQRuMGowROYIKwYBBQUH
MAKGOWh0dHA6L y9jYS5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LWVjYzM4NGVhZGR2b3YyMDE5
LmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZWFkdHJ1c3QuZXUwHQYDVR0lBBYwFAYIKwYB
BQUHAwEGCCsGAQUFBwMCMAoGCCqGSM49BAMDA2cAMGQCMFqnk4zWsC5s5l+6abjGtJHRJBkaGeCJ
zs7CXXWBDFEF3Wcv9b1zKCjr2IZb8hkLZAIwRDNBSURcXnoz1GgWrmW/dazQkfc+VTQ7t15/sSrm
crCU/mBTjo5llrCWFbMV/HgS

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer C:	*ES*
Issuer O:	*European Agency of Digital Trust, S.L.*
Issuer CN:	*EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019*
Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019*
Valid from:	*Thu Jun 06 13:35:55 CEST 2019*
Valid to:	*Tue Jun 03 13:35:55 CEST 2031*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:EA:8E:31:3B:33:F3:1F:61:ED:F5:62:B8:EF:AB:C4:62:3E:A7:90:2D:C6:89:8A:26:2F:D6:12:46:ED:20:CD:D8:B6:A1:29:66:F1:E6:5C:18:4B:83:EE:97:B4:19:DD:D8:F0:92:FB:03:5C:A0:47:32:14:6B:E4:D4:B9:FB:4F:8C:1E:0C:7D:62:F3:EF:D5:5C:1D:90:91:C6:D1:59:AF:14:6E:7A:C8:78:1C:DE:B5:85:A3:EA:92:4E:EC:15:25:31*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401* *CPS pointer: http://policy.eadtrust.eu*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*66:3F:D5:EB:2C:B0:D1:CF:E4:73:E6:17:C0:68:C5:73:EA:6F:F6:4A*
Authority Key Identifier	*1C:94:D8:12:94:49:7F:D7:AD:43:71:BB:2E:B2:BA:33:D2:C0:F4:46*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-root-ecc384eaddvov2019.crl*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-root-ecc384eaddvov2019.crt* *http://ocsp.eadtrust.eu*
Extended Key Usage	*id_kp_serverAuth*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*80:AB:1B:AA:C5:CA:A2:36:E8:80:17:92:FF:C8:8D:DC:CE:45:A9:30:FA:30:E5:78:DB:94:4D:51:28:2E:15:70*

X509SubjectName

Subject C:	*ES*
Subject O:	*European Agency of Digital Trust, S.L.*
Subject CN:	*EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019*

X509SKI

X509 SK I *Zj/V6yyw0c/kc+YXwGjFc+pv9ko=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.16.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.17 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019*

Name *[es]* *Certificados cualificados emitidos por EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7234582286219883415*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHK2CCBROgAwIBAgIIZGZmQkR4M5cwDQYJKoZIhvcNAQELBQAwgYQxRDBCBgNVBAMMO0VBRFRy
dXNlIFJTQSBzb0MDk2IFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIgRFYvT1YgQ2VydCAyMDE5MS8w
LQYDVQQKDCZFdUJvcGVhbnBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMC
RVMwHhcNMTkwNjA2MTEyNDE0WhcNMzEwNjAzMTEyNDE0WjCBgjFCMEAGA1UEAww5RUFEVHJ1c3Qg
UlNBIDQwOTYgU3ViQ0EgRm9yIFF1YWxpZmllZCBXZWIgRFYvT1YgQ2VydCAyMDE5MS8wLQYDVQQK
DCZFdUJvcGVhbnBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCwSqngVOtys8szrKDeMCvgqHgQyX3HAt02ifan
OGpBFbEpZcZTs8y7ueKj5t6BVHPIEcvQoIUR7202L9Iz2Tnj6yIWF6vwvrtuKF4vOy3PUJMohrFO
AGGfwOBcltSmfY09jNQoIWBlG25cxLYIEa2WCSVYzolaPiO9Az/BMTZBm87RgIUqls+6SDPAyA6
ZUcERziKZaK1zAGS51SaDaDYhktApjbtFvO55cIX7QXvbQes8EuR1.6S/FDTWRWkGiUUvITZKqAZ
nNU/9ZnjCmoV5gD7Gv2QeQgpzDSyDP3ZdMKWOhA1cS65sP0s+Oy+tv9ORzjYQ0jog70ECVg1i1
aNQR6sT3tdi2PN1UDPLNGoXtUDAsmrsNC97X0nj0LSLw+8HxjZFB77cXy5KvneoobNg8z8u/1IDU
IO+3XdRym6uk3HLXyJTaYpZwn/F6NrzgSnwhvR/s2FMjO+cdEUfyyGOJczU9PmxYp0vDU94etdWY
FTRel037MO79Td3W7fSOhfhwHSO4SAycVXJI0foCdHRcVPH0GigBVQmrh2zH80dmZcmFeNOTqrc7v
4GyLI54ZNw9kK0RzhlrnjDIVRsU3FtmDV2PNvkSCtrZyJdFXWnXbITaA92eSa8b6Knb+tbO0hmnb
obUaw/XJI1r9TEuGegl4UHlqPZ52daBEQ51eQQIDAQABo4IBnzCCAZswSwYDVR0gBEQwQjAGBgRV
HSAAMDgGDSsGAQQBg3UCAQEBgxEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5lYWR0cnVz
dC5dTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUUGru8dcf
pa8oIo6W5AMAn884urLcwHwYDVR0jBBgwFoAUIsV5nbYchdlSHcscdojFLMmvDUcwTAYDVR0lBEUw
QzBBoD+gPYY7aHR0cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LXJzYTQwOTZlYWRk
dm92MjAxOS5jcmwwewYIKwYBBQUHAQEEbzBtMEYGCCsGAQUFBzAChjpodHRwOi8vY2EuZWFkdHJ1
c3QuZXUvZWFkdHJ1c3Qtcm9vdC1yc2E0MDk2ZWFkZHJ2vdjIwMTkuY3I0MCMGCCsGAQUFBzABhhdo
dHRwOi8vb2NzcC5lYWR0cnVzdC5ldTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJ
KoZIhvcNAQELBQADggIBAG0egb6nmyfLyVdrWKg2Cszu8pSEV5xWAw4AvID5ruZ6DNp4VMYBEHK
NiY2EQFCOII1Gg79B2oYUwRXzD6lKorN3zisx0dnn8fvpwv+kWTI2LyJUlRtyv0/Vg/orE/ZNVtE
qrnY7hcGiFh+KuIw8uN84TusMCDoLDxVVb+0lYmhEjN3S6y9Gjp41KK4Hw2Ou4RBmJSv5D7HZibg
WVowWEk2sdntO319YTbRC3A+3jAK2CKRPmZvkBFuIDXFbHi3Bd7qnt80yOsxN+Fig/Ej8+F+ClbS
+97KAngAS8L0uRH19CW/4/ogA8ypH1TScQLWPehRFwVOlC1S0AmP6rGM+OEK3vpFsRtP0kHHBROs
5Mmtek3CFssdXal7fZZJs2l2HQ1MM/OgplNSKHku/soVC8bTdN5g5+yrUStdURRIjgkDxQCuyqX
FcJf29smDzGCwQ2y7RSgLs0Qr0uasDojS92r3BPrp/hFvvlkjsN4IvfgArnjfndzEiubf4IgUT8d
oxadAgHect64fMWlkWdtns3cVFmvg9lySzKRWe5KIWVO2NymeuryRbRVaY2dVYBr1ARFcX4Nv1I0
apLGrAmJxRD4eIDNuDczE1T2EvVaK0l68W90I5WYACn0+eQCAworop0lXK12YcsaaRKd3NhlVrDx
jv1Dg1sLTsbhUFv2RvQK

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 4096 Root CA For Qualified Web DV/OV Cert 2019*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019*

Valid from: *Thu Jun 06 13:24:14 CEST 2019*

Valid to: *Tue Jun 03 13:24:14 CEST 2031*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B0:4A:EA:60:54:E8:AD:CA:CF:2C:CE:B2:83:78:C0:AF:82:A1:E0:43:25:F7:1C:0D:36:89:F6:A7:38:6A:41:15:B1:29:
65:CD:93:B3:CC:BB:B9:E2:A3:E6:DE:81:54:73:C8:11:CB:D0:A2:55:11:EF:6D:36:2F:D2:22:D9:39:E3:7F:22:16:17:AB:F0:BE:BB:6E:28:5E:2F:3B:2D:CF:50:93:28:86:B1:4E:00:61:9F:C0:E0:5C:96:D4:A6:7D:8D:3D:8C:D4
:28:95:60:65:1B:6E:5C:C4:B6:08:11:AD:96:09:25:58:CE:89:5A:3E:28:8E:F4:0C:FF:04:C4:D9:06:6F:3B:46:02:14:A8:8B:3E:E9:20:CF:03:20:3A:65:47:04:47:38:8A:65:A2:B5:CC:01:92:E7:54:9A:0D:A0:D8:86:4B:6D:02:98:
DB:B4:5B:CE:E7:97:25:5F:B4:17:FE:14:1E:B3:C1:2E:44:BE:92:FC:50:D3:59:15:A4:1A:25:14:BC:84:D9:2A:A0:19:9C:D5:3D:66:78:C2:9A:85:79:80:3E:C6:BF:FC:D0:78:E8:29:CC:34:B2:0C:FD:D9:74:C2:96:39:B0:35:71:
2E:B9:B0:FD:2C:F8:EC:BE:B6:FF:4E:45:E8:D8:42:58:E8:8E:0E:F4:10:2F:D5:83:58:B5:68:D4:11:EA:C4:F7:B5:D8:B6:3C:DD:54:0C:F2:CD:1A:85:ED:50:30:2C:9A:BB:0D:0B:DE:D7:D2:78:F4:2D:22:F0:F9:FB:07:C6:36:4
5:07:BE:DE:5F:2E:4A:BE:77:A8:84:D8:3C:CF:CB:BF:D6:50:D4:20:EF:B7:5D:D4:72:9B:AB:A4:DC:72:D7:C8:94:DA:62:96:70:9F:F1:7A:36:BC:E0:4A:7C:21:BD:1F:EC:D8:53:23:3B:E7:1D:11:47:F2:C8:63:89:73:35:3D:3
E:6C:58:A7:4B:C3:53:DE:1E:B5:D5:98:15:34:5E:97:4D:FB:30:EE:FD:4D:DD:D6:ED:F4:8E:85:F8:70:1D:23:B8:48:0C:9C:55:72:48:D1:FA:02:74:74:5C:54:F1:F4:1A:00:55:42:6A:E1:DB:31:FC:D1:D9:99:72:61:5E:34:EE:E
A:AD:CE:EF:E0:6C:8B:97:9E:19:37:0F:64:2B:44:62:6E:5A:F0:8C:32:55:46:C5:37:16:60:D5:D8:F3:6F:91:20:AD:8B:F6:72:25:D1:57:5A:65:E1:95:36:80:F7:67:92:6B:C8:7A:2A:DB:DB:FA:D8:4E:F6:79:A1:A1:B5:1A:C3:F
5:C9:97:5A:FD:4C:4B:86:7A:09:78:50:79:6A:3D:9E:76:75:A0:44:43:9D:5E:41:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: http://policy.eadtrust.eu

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *50:6A:EE:F1:D7:1F:A5:AE:28:0F:A5:B9:00:C0:27:F3:CE:2E:AC:B7*

Authority Key Identifier *B6:C5:79:9E:16:1C:85:D9:52:1D:CB:1C:D2:88:C5:2C:C9:AF:0D:47*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa4096eaddvov2019.crl*

Authority Info Access

http://ca.eadtrust.eu/eadtrust-root-rsa4096eaddvov2019.crt

http://ocsp.eadtrust.eu

Extended Key Usage *id_kp_serverAuth*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *07:2C:23:9E:48:EE:41:17:F2:79:35:1A:1F:39:E2:B2:C8:5A:34:DA:65:52:43:EF:FF:18:D9:9B:CB:10:F9:14*

X509SubjectName

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019*

X509SKI

X509 SK I *UGru8dcfpa4oD6W5AMAn884urLc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.18 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019*

Name *[es]* *Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *2461622916454388023*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIILKzCCBxQgAwIBAgIIIikABI5kTcwDQYJKoZIhvcNAQENBQAwgYQxRDBCBgNVBAMMO0VBRFRy
dXN0IFJTQSA4MTkyIFJvb3QgQ0EgRm9yIFF1YWxpZmllZCBXZWIgRFYvI1YgQ2VydCAyMDE5MS8w
LQYDVQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMC
RVMwHhcNMTkwNjA2MTEzMzM0WhcNMzEwNjAzMTEzMzM0WjCBgjFCMEAGA1UEAww5RUFEVHJ1c3Qg
UlNBIDgxOTIgU3ViQ0EgRm9yIFF1YWxpZmllZCBXZWIgRFYvI1YgQ2VydCAyMDE5MS8wLQYDVQQK
DCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMwggQi
MA0GCSqGSIb3DQEBAQUAA4IEDwAwggQKAoIEAQCx1dSR8NTUNMTLAuISQ9r9zLrUDRrqVRVJmJ
ydIrfL8TSlAkS0OHE1ai1QLZ/YWlqwI8MzLGisp+aMQGZlkNpqJ0WHrg/XX0tMyes54K0g8GLPRt1
DwKv9KPltu63EKrBTh7a0OlkzEhFlhlvzgbvLBdjaf19y7z9IOA/mmmu7KS/MzduOTn9A4I3ATdV
6osE2vIkmS+fAoooHe4koCBbS+iKUHnD7x0dctq7ytwP0FF/WqyT64bX8uogn7krRBzf48Bvh/eb
I16rzRbt9g4VzxtokT7GfcGEHIwtNKKwvMRBTmIM4nLqcl88Ov9kIn3ueQhMTLiB0pquevmjlk
hn4Zhl121Xd1rZSg8qDh1dCABFwaqNpzhaeBKdViE3mDDhO5KywB2nIT/rNUSyj2Qz+19SAtZ7W
pS3FkYp71EmrTAYnQ7vdqeY/4EiCELEGzJP+yb36U/PbbCJ2EupH20zH1PmCxwNXb5O6Zb0ZoI7nB
4xBZFrKyKWvSo2lvs3KhckyqAFDSWH81vLDguXxohKt7OPMDzJKKTzu2dvcVSgla2EYr6Sq5F+aY
80MTFFuxOuP+DsjNdJIBxcsdp8WfrVab3yrLaHan7XdqFHRW0SdBhK+yRRgUSdjN/4iDD2vg+bp
GfaFbmfGt6U32hKCToj7nNOjRGT58U/bISmy7wxCnYnjnKQLs8nGcLxHdlvizzHDJYf1wnel6s2y
iwhD5L1SrH85Yr5lGVZJUO0VyYQs6WQ0ZFoxA1TuCwAQhsmx4P+XJ5TxkFhFAcF0Bvebt0qT6Rw8N
/HvDtge3UpN848/U1tbi1434K584pqJHTqEhEIRP9ZqBQgy1j+TRPXX234aA147rAYMO+FteeVP
AxcZbf+cWrj2iIEPUYSs2Dl4DJ7LXBIzdRJ83bGoKvZcSPuPst1GvW8Qh5Ie9DeS0S7uAWLeYFVJu
8hIAHTRau1sfLGolivKLsc1p8iy93DushjiID4+RsE5FN/6coq/pprxA6qwnhWWLKdkgyRNJxa8r
P9/fW4vQiI+7kfqFGM8j17b/iHpXzoiHbrXPM+gGWyZZ/MJlTodFLNq5jZup+6+1S2S/sYBhAI8f
AM67KNDstO08VkGpXjSHIJm6QA4pwcLLhCd2aClzwdEWO30+wwuS+7tpneP4P78r1ECNnrAgpUBV
YKF5F+2b7xOiZu6LfzIA0Ri1TKfkVPGUVGiSwKrFzUvFsyzSMaD/9C9poKioYmuBjNMJnYiLIIws
pS5TQaUAd0gIUXwIKJaLJ1ncsn5jntAv+OCzvcSSZOxD2PaaStQNr0Bm6PccUvUIu1hm8se7YTXI
QnJtGP8us3tfFq1IXRIV8RqHPSB6KLlIAIfjAgMBAAGjggGtMIIBmzBLBgNVHSAERDBCMAYGBFUd
IAAwOAYNKwYBBAGDdQIBAQGDETAnMCUGCCsGAQUFBwIBFhlodHRwOi8vcG9saWN5LmVhZHRydXN0
LmV1MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdDgQWBBRRzoY4OeBX
ojWZsYyyV2WKyn57TTAIBgNVHSMEGDAWgEBSc7QxBgWpv+mYJ+nx/iEhjCDZ9ADBMBgNVHR8ERTBD
MEGgP6A9hjtodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRydXN0LXJvb3QtcnNhODE5MmVhZGR2
b3YyMDE5LmNybDB7BggrBgEFBQcBAQRvMG0wRgYIKwYBBQUHMAKGOmh0dHA6Ly9YS5IYWR0cnVz
dC5ldS9lYWR0cnVzdC1yb290LXJzYTgxOTJlYWRkdm92MjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0
dHA6Ly9vY3NwLmVhZHRydXN0LmV1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkq
hkiG9w0BAQ0FAAOCBAEAulcF47Uj9RVS4rdUSpbjPvc5mB4843uhTTCE1NwGC+uQpKMk+JNG968i
Rbv2I1aJFz6Rdb0FcXyqN5ppo9ry+aHG4fMNzjGNbVUq77Ua1NAQ9uWUHMFDBH5Qm05StXuGwbHd
quwZoP6PEpYzBpET/UmwUNzjR8HG9SYEs+kPG63xxN0R6gynM+aYQPAut+IA/oMrrBcEavYggj9X
yJTbHpRj5/b1LYc7CA6J5rnS8P9BQPYGnO9M5YWrKdZuuYZnvu91uy7pcbU/izt0IuKbV9GBHzsvEU
tSis/5cWq7jI6CMzhP9AOnq35KZI3weyDyw3I7knMZhJlXJt0e7OQds27TDCJWgS6bsY/YBeg1u
ZI2xkBtZEc6NDcV2312luvI93uqygzSZKOjTm1EQEyhr7UlCxcqYO9j+CtnoIH4ng/iXAKjon2vc
4fM3jVmauiITk4JmQuXRYiuyUJxBP2vNmtbVCQ8mSNUbHucZGQAisNdq7DvdSdlXsLKEv4V8Cp9vE
hWZ+0tHKUAhTcychOhE1HnxgrmrD0tnfSIOMSxuIPMdjJmRyacVUpF2UlGQnOnCTsuBgyAuX8zrLX
Elhg+VZLZ6ZqN1ZeuRQ4F1KKX+jm6zmj6pV8dXvs/sl/ahgIxQAmhj4+MQY3lq0kLUkw2h1PKG7Dy
/iAvcPXyadH92lZQgztPQTKn7J5VvJF7P8w6HbbXa5EmlP3nnISiuuPhxS/q+2VVhuVm48iCI891
3CA82hiYKkv7lXGV9Ba4nu07YODnw4tJW8SX/WlO72PLQEM85kljeANbVQG0T4/sgDqlQKaVdgaYy
taubrTpiVXgkatQBIXtCI6TL1mruPGiy7NHmuPfe+/RFxsEYkJ7QZ2PEB0K9jEVCc2ZpIG7Nmg8+
eXVUQrEe41MjwkYrmAbHnqd7mQFovXUrg4QThhcBXE08TIvDHiD2PZAyJWE+dZBgKChbV1l/hsT
MUaphKFz1Rrvk6CPhs46AaFvbcVeeYJyOldyc3/EJXta/bsRVONbGiVkspkweD2JwBjSRy/FwKs0
oHGpBETRbOC9b2VXKC7wpfyt6JeDKK1TRKR0cH94oOuD6Q1em5phpSH+CEXogdJCwpYM1nTha0N
FuYSfBC/zpU1PtAWS1tt8e9YKoBfiaTcpvUtv6pnrBeOyC4Z24nLJtobxGNz/lapsRwKAJi6DTA
Eyyk3PA3QgyZrza6fCN8qDsJcp0Hbz5zr5yanIIrsTvQz+dNk1XKni865CfeZLa4o1LrNbCU/6kWF
JcGjlmvyblRnbAGo6+J6PAJ674ctL5ONS4DE9bMkv7MwA9rhasvnrrUirfyVUJB4szSbVhnWF2L1
0inGqOif3hMZETXbaQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 8192 Root CA For Qualified Web DV/OV Cert 2019*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019*

Valid from: *Thu Jun 06 13:33:34 CEST 2019*

Valid to: *Tue Jun 03 13:33:34 CEST 2031*

Public Key:

30:82:04:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:B1:D5:D4:91:7F:C7:D3:FD:43:4C:4C:B0:2E:21:24:3D:8B:DC:CB:AD:40:D1:AE:A5:51:54:99:89:C9:D2:2B:7C:BF:13:48:80:24:4B:43:87:13:56:A2:D5:02:D9:FD:85:89:AB:02:3C:33:32:C6:8A:CA:7E:68:C4:06:66:59:0D:A6:A2:74:58:7A:E0:FD:75:F4:B4:CC:9E:E7:82:B4:83:C1:8B:3D:1B:75:0F:02:AF:F4:A3:E5:B6:2E:B7:10:AA:C1:4E:1E:DA:D0:E9:64:CC:48:45:22:18:6F:CE:06:EF:2C:17:63:69:F2:3D:CB:BC:FD:20:E0:3F:9A:79:AE:EC:AB:3F:33:37:6E:39:39:FD:03:82:37:01:37:55:EA:8B:04:DA:F2:24:99:2F:9F:02:2A:28:1D:EE:24:A0:20:5B:4B:E8:8A:50:79:C3:EF:1D:1D:C6:DA:BB:CA:DC:0F:D0:51:7F:5A:AC:93:EB:86:D7:F2:EA:20:9D:39:2B:44:1C:DF:E3:C0:6F:87:F7:9B:97:57:E8:AC:44:61:F6:0E:38:57:3B:68:93:B4:C6:7D:C1:84:1E:FC:2D:34:A2:B0:BC:C4:41:4E:62:0C:E2:7F:CB:A9:C9:7C:F0:EB:FD:90:89:F7:B9:E4:22:30:52:E2:07:4A:6A:8A:E7:AF:9A:39:64:86:7E:19:86:5D:76:D5:77:75:AD:94:A0:F2:A0:E1:D5:D0:80:04:5C:1A:A8:DA:73:85:A7:81:29:D5:62:13:79:83:0E:13:B9:2B:2C:01:DB:32:13:7F:FA:CD:51:2C:A3:D9:0C:FE:D7:D4:80:B5:9E:D6:A5:2D:C5:91:8A:7B:D4:49:AB:4C:06:27:43:BB:DD:A9:E6:3F:E0:48:82:10:B1:06:AC:93:FE:C9:BD:FA:50:F6:DB:08:9D:84:BA:91:F6:D3:31:F5:3E:60:B1:C0:D5:DB:E4:EE:99:6F:46:68:23:B9:C1:E3:10:59:16:B2:B2:29:6B:FC:A3:69:6F:B3:72:A1:72:4C:AA:00:50:D2:58:7F:35:BC:B0:E0:B9:7C:68:84:AB:7B:38:F3:03:CC:92:8A:4F:3B:B6:76:F7:15:4A:09:5A:D8:46:2B:E9:2A:B9:17:E6:98:F3:43:13:14:51:6E:C4:E6:8F:F8:3B:23:35:D2:09:06:27:2C:76:9F:16:7E:B5:5A:87:7C:AB:2D:A1:DA:9F:B5:DD:A8:51:D1:5B:44:9D:06:12:BE:C9:14:60:51:27:63:37:FE:22:0C:30:EF:83:E6:E9:19:F6:85:6E:67:C6:B7:A5:37:DA:12:82:4E:88:FB:9C:D3:A3:44:64:F9:F0:9F:DB:7D:29:B2:EF:0C:42:9D:89:E3:9C:A4:0B:B3:C9:C6:70:BC:47:74:8B:E2:CF:31:C3:25:87:F5:C2:77:88:EA:CD:B2:8B:08:43:E4:BD:52:AC:7F:39:62:BE:65:19:56:49:53:45:72:61:0B:3A:59:0D:19:16:8C:40:D5:3B:82:C0:04:21:B2:6C:78:3F:E5:DF:27:94:F1:90:58:45:01:C1:74:06:F7:9B:D2:A4:FA:47:0F:0D:FC:7B:C3:B6:07:B7:52:93:7C:E3:CF:D4:D6:D6:E2:D7:8D:F8:2B:9F:38:A6:A2:47:4E:A1:21:11:F4:4F:F5:9A:81:42:0C:B5:8F:E4:D1:3D:75:F6:DF:86:80:D7:8E:EB:01:83:0E:F8:5B:5E:7A:D5:4F:03:17:99:6D:FF:9C:5B:38:F6:8A:51:0F:51:84:9A:D8:39:78:0C:9E:CB:5C:12:33:75:12:7C:DD:B1:A8:2A:F6:5E:48:FB:8F:C6:DD:46:BD:6F:0E:B5:29:3D:0D:E4:B4:4B:BB:80:58:B7:98:15:52:6E:F2:12:00:1D:34:5A:BB:5B:1F:2C:6A:25:8A:F2:8B:B1:CD:69:F2:2C:BD:DC:3B:AC:86:38:88:0F:8F:91:B0:4E:45:37:FE:9C:A2:AF:E9:A6:BC:40:EA:AC:27:85:65:8B:29:D9:20:C9:13:49:C5:AF:2B:3F:DF:DF:5B:8B:D0:88:8F:BB:91:FA:85:18:CF:23:D7:B6:FF:88:7A:57:CE:88:87:6E:B5:CF:33:E8:06:5B:26:59:FC:C2:65:4E:87:45:2C:DA:B9:8D:9B:A9:FB:AF:B5:4B:64:BF:B1:80:61:02:5F:1F:00:CE:BB:28:D0:EC:B4:ED:3C:56:41:A9:5E:34:87:20:99:BA:40:0E:29:C1:C2:CB:84:27:76:68:29:73:C1:D1:16:3B:7D:3E:C3:0B:92:FB:BB:69:9D:E3:F8:3F:BF:2B:D4:40:8D:9E:B0:20:A5:40:55:60:A1:79:17:ED:A1:EF:13:A2:66:EE:88:66:27:C0:D1:18:B5:4C:A7:F1:54:F1:94:54:6F:F9:C0:AA:C5:CD:4B:C4:CA:CD:92:31:A0:FF:F4:2F:69:A0:A8:A8:63:F9:9A:06:33:4C:1E:74:E2:2C:7C:2C:A5:2E:53:41:A5:00:77:48:25:51:7C:08:28:96:8B:8F:59:DC:B2:7E:63:9E:D0:2F:F8:E0:B3:BD:E4:92:64:EC:43:D8:F6:9A:4A:D4:0D:AF:40:66:E8:F7:9C:52:F5:25:BB:58:66:F2:C7:BB:61:35:E5:42:72:6D:18:FF:2E:B3:78:9F:16:AD:65:5D:12:15:F1:1A:87:3D:20:7A:28:B9:48:00:87:E3:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: http://policy.eadtrust.eu

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

51:CE:86:38:39:E0:57:A2:35:99:B1:8C:63:57:65:8A:CA:7E:7B:15

Authority Key Identifier

9E:ED:0C:41:81:6A:6F:FA:66:09:FA:7C:7F:8C:48:63:08:36:7D:00

CRL Distribution Points

http://crl.eadtrust.eu/eadtrust-root-rsa8192eaddvov2019.crl

Authority Info Access

http://ca.eadtrust.eu/eadtrust-root-rsa8192eaddvov2019.crt

http://ocsp.eadtrust.eu

Extended Key Usage

id_kp_serverAuth

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

A1:46:16:D1:E8:C0:B4:9E:0E:21:CA:E2:B5:42:A8:35:1A:26:74:7D:3A:18:A4:59:99:C3:8B:A1:D0:78:B6:CB

X509SubjectName

Subject C:

ES

Subject O:

European Agency of Digital Trust, S.L.

Subject CN:

EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019

X509SKI

X509 SK I

Uc6GODngV6I1mbGMY1dlisp+exU=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.18.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.19 - Service (granted): Qualified timestamps issued by QTSU ALPHA EADTrust

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified timestamps issued by QTSU ALPHA EADTrust*
Name	*[es]*	*Sellos electrónicos cualificados de tiempo emitidos por QTSU ALPHA EADTrust*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *11997848830949807878 42*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIITTCCBjWgAwIBAgIJQQpcKnEv5f6CMA0GCSqGSIb3DQEBCwUAMIGxMUAwPgYDVQQDDDdFQURU
cnVzdCBSU0EgNDA5NiBTdWJDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmljYXRlcyAyMDE5MS8wLQYD
VQQKDCZFdOvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5ML jELMAkGA1UEBhMCRVMx
GDAWBgNVBGEMD1ZBVEVTLU4NTYyNjI0MDEVMBMGA1UECwwMTGVnYWwgUGVyc29uMB4XDTE5MTAx
ODExMTEyN1oXDTIzMTAxNzExMTEyN1owgZ8xHDAaBgNVBAMME1FUU1UgQUxQSEFgRUFEVHJ1c3Qx
IDAeBgNVBAsMF0VudGl0eSBTZWFsIENlcnRpZmljYXRlMRgwFgYDVQRbDA9WQVRFUy1CODU2MjYy
NDAxNjA0BgNVBAoMLUVBRCBUUlVTVCBFVVJPUEVBTiBBR0VOQ1kgT0YgREIHSVRBTCBUUlVTVCBT
TDE1MAkGA1UEBhMCRVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEgGGDntaH22S/
NX5QJGOOTysPglezNvTIq7yJVIZIVHNLIpyZU2/P/RijUZbJCfsOLk1wQInwS7zfU1aONsxcsJl4
GCJU3bnK2sujrjfccX+inuxYvu0tDq3EVXI9iEhd2KaJb29AURyTlat+ENNvYyxYJQvbTQ86kU7H
cyvtKB/rQFF4ahkCvP9j0SVJToaazkB3k6dThkCDfQcjPg2L1xwA/DAfwbWY0lflU/8ScKUbnCt8
RRPs0TUAufsdv8QycO8u2etKAemTEvEs/MEEY0bcWxn4kTiHsheeyf5OJEBXsWUgbDrHk4Gol
J68X2aIREODjBn3JwaGxPB/AgMBAAGjggN2MIIDcjATBgNVHSMEGDAWgBQxLIvaS/Z6y/blDgJ
44SnLEn/RTB6BggrBgEFBQcBAQRuMGwwRQYIKwYBBQUHMAKGOWh0dHA6Ly9jYSSlYWR0cnVzdC5l
dS9lYWR0cnVzdC1zdWJjYS1yc2E0MDk2ZWFkbHAyMDE5LmNydDAjBggrBgEFBQcwAYYXaHR0cDov
L29jc3AuZWFkdHU1c3QuZXUwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cu
ZWFkdHU1c3QuZXWGFWh0dHA6Ly9YSS1YWR0cnVzdC5ldYZaHR0cDovL3BvbGljeS5lYWR0cnVz
dC5ldTBmBgNVHREExzBdgQ5jYUBlYWR0cnVzdC5ldYWaHR0cHM6Ly9jYSS1YWR0cnVzdC5ldYYX
aHR0cHM6Ly93d3cuZWFkdHU1c3QuZXWGGmh0dHBzOi8vcG9saWN5LmVhZHRydXN0LmV1MIIBEwYD
VR0gBIIBCjCCAQYwgZIGDSsGAQQBg3UCAQEBgyUwgYAwVwYIKwYBBQUHAgIwSwzJRXVyb3BlYW4g
QWdlbmN5IG9mIERpZ2l0YWwgYHU1c3QsIFMuTC4gTGVnYWwgtLGVyc29uIFI1YWxpZmllZCBDZX0
aWZpY2F0ZTAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBvBgcEAIvsQAED
MGQwYgYIKwYBBQUHAgIwVgxURXVyb3BlYW4gVGVsZWNvbW11bmljYXRpb25zIFN0YW5kYXJkcyBJ
bnN0aXR1dGUuIGVJREFTIEV1cm9wZWFuFIJZ3VsYXRpb24gQ29tcGxpYW50MBYGA1UdJQEB/wQM
MAoGCCsGAQUFBwMIMFsGCCsGAQUFBwEDBE8wTTAVBggrBgEFBQcLAjAJBgcEAIvsSQECMAgGBgQA
jkYBATALBgYEAI5GAQMCAQ8wCAYGBACORgEEMBMGBgQAjkYBBjAJBgcEAI5GAQYCMEsGA1UdHwRE
MEIwQKA+oDyGOmh0dHA6Ly9jcmwuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtc3Vi Y2EtcnNhNDA5NmVh
ZGxwMjAxOS5jcmwwHQYDVR0OBBYEFOJgGRCp+XB1YEs3rNYSnkfcom4CBMA4GA1UdDwEB/wQEAwIH
gDANBgkqhkiG9w0BAQsFAAOCAgEAPLDMQIALtG9/2TId2lNVZzy6ioRO7sAnce2UNmX3zIrIB1
6dKjtcKx2MnFfQtxcsRbwpO4xjfPRD219SiAzKBwbe8DhacEpXVea62pbl32WVCLsuu2GlY0CWLC
cimhjrimEzJPpAUYJeh80HtPFLKbjW2vyZt3HVvv9UYuPObj+H/UJLdDNzbM1gy0c1N49+BCBw8w
s+qr1sHnc83rf63NBONZ3yt+G5X6mG2l77uJOyB6YpTW0xcpcnOOBMVmQOqgKS3KfU+RbWpulDuO
8xpCYYXMVuoEkPYaI7l4Iocc++v16WfzQuI2F2KiIIeuwyANYgs5U3RZ5BwNAcoiX233bmSicOIa3
1uzQL5VhZGVegZVyOu5l4dIBJqIK23InLmRtP0tlRr1jKN/cuxW6mvXpvhXcHb7rXs24HaocW
58l9p2dj6L15iZ9pkJLNBcNy1q2b9mdR4q9b65kRbBUYV0Y9KVSwIiTL4SYf1r32CcNV70T4auvm
yp2NR523w823nj2OQT1vz4lzYkIJw+P6N+ryQvCx5YwcXcBU3CfMEcafPcSNKJN6DGa7gOWoj+SS
0TwdL4b7d5Yy0iRcQ1TGuocqPdpOmIA0mu8HJ64zXsrRcahSXml/7b7Hvhhh6hozkoimHtS8O0m1
/ZSvZLDCzo120kL2uTiTIMMydy8=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *Legal Person*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C:	*ES*
Issuer O:	*European Agency of Digital Trust, S.L.*
Issuer CN:	*EADTrust RSA 4096 SubCA For Qualified Certificates 2019*
Subject C:	*ES*
Subject O:	*EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*
Subject 2.5.4.97:	*VATES-B85626240*
Subject OU:	*Entity Seal Certificate*
Subject CN:	*QTSU ALPHA EADTrust*
Valid from:	*Fri Oct 18 13:11:27 CEST 2019*
Valid to:	*Tue Oct 17 13:11:27 CEST 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C4:80:61:83:9E:D6:87:DB:64:BF:35:7E:50:24:63:8E:4F:2B:0F:82:57:B3:36:F4:C8:AB:BC:89:BF:56:48:54:73:4B:22:9C:99:53:6F:CF:FD:18:A3:51:96:C9:09:FB:0E:2E:4D:70:40:89:F0:4B:BC:5F:50:B6:8E:36:CC:5C:B0:89:78:18:22:54:DD:B9:CA:DA:CB:A3:8A:37:DE:71:7F:A2:9E:EC:58:BE:ED:2D:0E:AD:C4:55:72:3D:88:48:5D:D8:A6:89:6F:6F:40:51:1C:93:95:AB:7E:10:D3:6F:63:2C:58:25:0B:DB:4D:0F:3A:91:4E:C7:73:2B:DF:28:1F:EB:40:51:78:6A:19:02:BC:FF:63:D1:25:49:4E:86:9A:CE:40:77:93:A7:53:86:40:83:7D:07:23:3E:0D:8B:97:1C:00:FC:30:1F:C1:B5:98:D2:57:E5:53:FF:12:70:A5:1B:9C:2B:7C:45:13:F1:D1:35:00:6A:27:F2:76:FF:10:C9:C3:BC:BB:67:AD:28:07:A7:89:31:2F:12:CF:CC:10:46:34:6D:C5:B1:9F:82:A4:4E:21:EC:85:E7:B2:7F:93:89:10:15:EC:59:4A:9B:0E:B1:E4:E0:6A:25:27:AB:7C:5F:66:88:44:43:83:8C:19:F7:27:06:86:C4:F0:7F:02:03:01:00:01*
Authority Key Identifier	*31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt* *http://ocsp.eadtrust.eu*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *https://ca.eadtrust.eu* *https://www.eadtrust.eu* *https://policy.eadtrust.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.501.2.1.1.1.421* *CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]* *CPS pointer: http://policy.eadtrust.eu* *Policy OID: 0.4.0.194112.1.3* *CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]*
Extended Key Usage	*id_kp_timeStamping*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15* *id_etsi_qcs_QcSSCD*

CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*
Subject Key Identifier	*E2:60:19:10:A9:F9:70:75:60:4D:EB:35:84:A7:91:F7:28:9B:80:81*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*92:E7:2C:68:F6:B8:4E:8C:71:4F:A6:A0:54:13:C8:D5:0B:8F:1A:97:73:EF:24:0A:17:B3:B0:B5:CA:59:8D:79*

X509SubjectName

Subject C:	*ES*
Subject O:	*EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*
Subject 2.5.4.97:	*VATES-B85626240*
Subject OU:	*Entity Seal Certificate*
Subject CN:	*QTSU ALPHA EADTrust*

X509SKI

X509 SK I	*4mAZEKn5cHVgTes1hKeR9yibgIE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*
URI	*[es]*	*https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.20 - Service (granted): Qualified time stamps issued by QTSU DELTA EADTrust

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified time stamps issued by QTSU DELTA EADTrust*

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por QTSU DELTA EADTrust*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1196650575481115087131*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIQDCCBiigAwIBAgIJQN7c3kYKoZEbMA0GCSqGSIb3DQEBCwUAMIGxMUAwPgYDVQQDDDdFQURU
cnVzdCBSU0lEgNDA5NiBTdWIDQSBGb3IgUXVhbGlmaWVkIENlcnRpZmljYXRlcyAyMDE5MS8wLQYD
VQQKDCZFdXJvcGVhbiBBZ2VuY3kgb2YgRGlnaXRhbCBUcnVzdCwgUy5MLjELMAkGA1UEBhMCRVMx
GDAWBgNVBGEMD1ZBVEVTLU4NTYyNjI0MDEVMBMGA1UECwwMTGVnYWwgUGVyc29uMB4XDTE5MTEw
NjExMDMyNloXDTIzMTEwNTExMDMyNlowgZ8xHDAaBgNVBAMME1FUU1UgREVMVEEgRUFEVHJ1c3Qx
IDAeBgNVBAsMF0VudG1fcSBTZWFsIENlcnRpZmlYXRlMRgwFgYDVQRhDA9WQVRFLy1CODU2MjYy
NDAxNjA0BgNVBAoML UVBRCBUUlVTVCBFVVJPUEVBTiBBR0VOQ1kgT0YgRElHSVRBTCBUUlVTVCBT
TDELMAkGA1UEBhMCRVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCCWAkAivA4C2rN
O7JNILhxhwFLsyAFLORoLaAijS9rr4XFc0LctObmb7z1vNh2HcyVCmUboNsm74EeUNbBGKjP912s
xsmpNSTLK2cscKdfo9mjATLX8tQPc3nQeiyr4fmk4okeUMlaM5yo7XCKIIlpgmj4RSStaUJbMOzkT
QS6ftl7PGAoLWuOSZmQgKW2wwIqYnojagOoRapkXAm0WkipgctKtLXzjMzp3qy6xJTHLJK94JsgHl
1jdmNpHldfQOI9b+gUtqd6uh9JpscrpwQdmu2fLQ2Df7zjfzM3/mmpTLOlD4cP276Ojmk1rXbXBi
PegyEWEDJ0Iv69ogAXJ9jxJVAgMBAAGjggNpMIIDZTAfBgNVHSMEGDAWgBQxLIfvaS/Z6ybIDgJ
44SnLEn/RTB6BggrBgEFBQcBAQRuMGowRQYIKwYBBQUHMAKGOWhkdHAtLy9YS5lYWR0cnVzdC5l
dS9lYWR0cnVzdC1zdWJyYS1yc2E0MDk2ZWFkbHAyMDE5LmNydDAjBggrBgEFBQcwAYYxaHR0cDov
L29jc3AuZWFkdHJ1c3QuZXUwYwYDVR0SBFwwWoEOY2FAZWFkdHJ1c3QuZXWGFmh0dHA6Ly93d3cu
ZWFkdHJ1c3QuZXWGFWh0dHA6Ly9YS5lYWR0cnVzdC5lYYZaHR0cDovL3BvbGljeS5lYWR0cnVz
dC5ldTBjBgNVHREEXDBagQ5jYUBlYWR0cnVzdC5ldYYVaHR0cDovL2NhLmVhZHRydXN0LmV1bkZo
dHR0cOi8vd3d3LmVhZHRydXN0LmV1bloidHRwOi8vcGVsaWN5LmVhZHRydXN0LmV1MlBEwYDVR0g
BIIBCjCCAQYwgZIGDSsGAQQBg3UCAQEAgyUwgYAwVwYIKwYBBQUHAgIwSwxJRXVyb3BlYW4gQWdl
bmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMuTC4gTGVnYWwgUGVyc29uIFF1YWxpZmllZCBDZXJ0aWZp
Y2F0ZTAlBggrBgEFBQcCARYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTBvBgcEAIvsQAEBMGQw
YgYIKwYBBQUHAgIwVgxURXVyb3BlYW4gVGVsZWNvbW1lbmlj YXRpb25zIFN0YWS3kYXRcysBlbnN0
aXR1dGUulGVJREFTIEV1cm9wZWFuIFJlZ3VsYXRpb24gQ29tcGxpYW50MBYGA1UdIQEB/wQMMAoG
CCsGAQUFBwMIMFEGCCsGAQUFBwEDBEUwQzAVBggrBgEFBQcLAjAJBgcEAIvsSQECMAgGBgQAjkYB
A TAL BgYEAI5GAQMCAQ8wEwYGBACORgEGMAkGBwQAjkYBBgIwSwYDVR0IBEQwQjBAoD6gPIY6aHR0
cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0cnVzdC1zdWJyYS1yc2E0MDk2ZWFkbHAyMDE5LmNybDAd
BgNVHQ4EFgOUqorTdJ7j/gRRMDskSfOJ40VQ0IwDgYDVR0PAQH/BAQDAgeAMA0GCSqGSIb3DQEB
CwUAA4ICAQA9GTyZZuScyK7x862GzW7U8G+YDVr8454DOae5tu5D7/cs0gjQOlpJsbL6UK1D1LQZ
Dpyl64L1lE4fYBTCYxY6sBVsph7fg8vmsmn0DywpcWrS0BtVCj7O+6mlZaToEIGE7Qk3zOlk09j
8SY9yTvqbdbKnxTUA8nyO3YbI3QDSsla+Q1IFNpArnlgcnZQabGfcQwd8jU3sTMRCre3WxX7bdJ
/K7I6yxlrj7WAPCaySm2f4LKhjc9/9vx+cVBhAeiLqlLfef0BclAjMSpOORZuZrEUrrh1Mt64D5S
6SIoKLV91ZyOmP1QWaRJnprlLSm9OdrvWCrahVcuzva55Isva8oS5RB08SZ5/IvuAoA6B2vRHubo
oJnCnqO9wcu33lmE4rcMMqO+Jl35OoiSUPTd2E+LQpKn16bAizQFN2X0ysc5+uDuv+2RAiIhpPWh
pEI8aMHBrudsq45FaW22UAkvYjr5ahI725AqNV1s5icuFD31MKAtuk+x/Q9wFIIs4ZtwD0FwVjwP
C5fpmZpKf1umBNTBqU/KoGc5PQWoGXpb2kT3b7rBs39sAskAoxyA8lrWiaDszUrDYUiVJeZ2/boE5
3H14GCh5sY+tX8I+DLR49pbMXIe5iWKXNudKR6nrSlXSV7e1LuzfCB6QV1k7m3xohOgPKzdbX/e2
cRliSEy/Mw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *Legal Person*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Entity Seal Certificate*

Subject CN: *QTSU DELTA EADTrust*

Valid from: *Wed Nov 06 12:03:26 CET 2019*

Valid to: *Sun Nov 05 12:03:26 CET 2023*

Public Key:

```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:82:58:09:00:8A:F0:38:0B:6A:CD:3B:B2:4D:20:B8:71:87:01:4B:B3:20:05:2C:E4:68:2D:A0:22:8D:2F:6B:AF:85:C5:7
3:42:DC:B4:E6:E6:6F:BC:F5:BC:D8:76:1D:CC:95:0A:65:1B:A0:DB:26:EF:81:1E:50:D6:C1:18:A8:CF:F7:5D:AC:C6:C9:A9:35:24:CB:6F:67:B1:78:A7:7A:A3:DC:23:01:32:FC:85:03:DE:DE:74:1E:8B:2A:F8:7E:69:38:A2:4
7:94:32:56:8C:E7:2A:3B:5C:22:88:94:8A:60:9A:3E:11:49:2B:5A:50:96:CC:3B:39:13:41:2E:A5:7F:53:C6:02:82:D6:B8:EE:59:99:08:0A:5B:6C:30:96:A6:27:A2:36:A0:3A:84:5A:A6:45:C0:9B:45:A4:8A:98:1C:B4:AB:4B:5F:
38:CC:CE:9D:EA:CB:AC:49:4C:72:DF:2B:DE:09:B2:01:E5:D6:37:66:36:91:E5:75:F4:0E:23:D6:FE:81:4B:6A:77:AB:A1:F4:9A:6C:72:BA:70:41:D9:AE:D9:F2:D0:D8:37:FB:CE:37:F3:33:7F:E6:9A:94:CB:3A:50:F8:70:FD:
BB:E8:E8:E6:93:5A:D7:85:70:62:3D:E8:32:11:61:03:27:42:2F:EB:DA:20:01:72:7D:8F:12:55:02:03:01:00:01
```

Authority Key Identifier	*31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt* *http://ocsp.eadtrust.eu*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://ca.eadtrust.eu* *http://www.eadtrust.eu* *http://policy.eadtrust.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421* *CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]* *CPS pointer: http://policy.eadtrust.eu* *Policy OID: 0.4.0.194112.1.1* *CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]*
Extended Key Usage	*id_kp_timeStamping*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*
Subject Key Identifier	*AA:8A:D3:74:92:7B:8F:F8:11:44:C0:EC:91:27:CE:27:8D:15:43:42*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*8F:04:72:62:CF:62:25:7E:BF:C8:85:E6:3F:65:11:12:31:35:13:3D:E2:8D:2A:8C:F1:03:4F:CC:B4:EA:7C:DA*

X509SubjectName

Subject C:	*ES*
Subject O:	*EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*
Subject 2.5.4.97:	*VATES-B85626240*
Subject OU:	*Entity Seal Certificate*
Subject CN:	*QTSU DELTA EADTrust*

X509SKI

X509 SK I *qorTdJJ7j/gRRMDskSfOJ40VQ0I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

40.21 - Service (granted): Qualified time stamps issued by QTSU EPSILON EADTrust

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified time stamps issued by QTSU EPSILON EADTrust*

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por QTSU EPSILON EADTrust*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *639936159653937015986*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGaDCCBVCgAwIBAgIJIrDl8q2ck+yyMA0GCSqGSIb3DQEBCwUAMIGeMUQwQgYDVQQDDDtFQURU
cnVzdCBSU0EgMjA0OCBTdWJDQSBGb3IgTm9uLVF1YWxpZmllZCBDZXJ0aWZpY2F0ZXMgMjAxOTEv
MC0GA1UECgwnRXVyb3BlYW4gQWdlbmN5IG9mIERpZ2l0YWwgVHJ1c3QsIFMu1C4xCzAJBgNVBAYT
AkVTMRgwFgYDVQRhDA9WQVRFUy1CODU2MjYyNDAwHhcNMTkzMTA2M1EwNDEzWhcNMjMxMTA1M1TEw
NDEzWjCBoTEeMBwGA1UEAwwVUVRTVSBFUFNJTE9OIEVBRFRydXN0MSAwHgYDVQQLDBdFbnRpdHkg
U2VbbCBDZXJ0aWZpY2F0ZTEYMBYGA1UEYQwPVkFURVMtQjg1Nj2MjQwMTYwNAYDVQQKDC1FQUQg
VFJVU1QgRVVST1BFQU4gQUdFTkNZIE9GIERJR0lUQUwgVFJVU1QgU0wxCzAJBgNVBAYTAkVTMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA01rjKvNGvvaNBzDBkUb/lV/AzBI1XBTTd1
qyqvQF6d4rcyxPgefb7ZvzwS/KOjHrUEoxGFfyRZsbtQwVK+HaiavI/NtNO8b6uigOd3eAVolphP
x1DNcws1tzev17Pm0Rfa0/1+zyXy3qZe7piDYDmE7Ul7y3uG9l117FCm1sIBh3nxBL1NDDnA91b8
O8R/kU2a5W3YgD3tnM5owmmODVdGP8PR1fkBLXIx+fDLejx5CXaCav0v/NsSs4TNi5KhswFcUBM0
6xMuEGXmbSHpPHg46g/E4pFFsCzgcWHXcszF+2g4xTWVkDQuINPKH08Shu T0cWZ0OUyYuzd0NjL
pwIDAQABo4ICojCCAp4wHwYDVR0jBBgwFoAU5+vpL3Lr+Vm9fVDpYhjQzybZFylweeYIKwYBBQUH
AQEEbjBsMEUGCCsGAQUFBzAChjlodHRwOi8vY2EuZWFkdHJ1c3QuZXUvZWFkdHJ1c3Qtc3ViY2Et
cnNhMjA0OGVhZG5xMjAxOS5jcnQwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVhZHRydXN0LmV1
MGMGA1UdEgRcMFqBDmNhQGVhZHRydXN0LmV1hhZodHRwOi8vd3d3LmVhZHRydXN0LmV1hhVodHRw
Oi8vY2EuZWFkdHJ1c3QuZXWGGWhtdHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwYwYDVR0RBFwwWoEO
Y2FAZWFkdHJ1c3QuZXWGFWb0dHA6Ly9jYS5lYWR0cnVzdC5ldYYWaHR0cDovL3d3dy5lYWR0cnVz
dC5ldYYZaHR0cDovL3BvbGljeS5lYWR0cnVzdC5ldTCBoAYDVR0gBIGYMIGVMIGSBg0rBgEEAYN1
AgEBAJhZMIGAMFcGCCsGAQUFBwICMEsMSUV1cm9wZWFuIEFnZW5jcSBvZiBEaWdpdGFsIFRydXN0
LCBTLiwuEsVZFsIFBlcnNvbiBRdWFsaWZpZWQgQ2VydGlmaWNhdGUwQYIKwYBBQUHAgEWGWh0
dHA6Ly9wb2xpY3kuZWFkdHJ1c3QuZXUwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwSwYDVR0fBEQw
QjBAoD6gPIY6aHR0cDovL2NybC5lYWR0cnVzdC5ldS9lYWR0cnVzdC1zdWJjYS1yc2EyMDQ4ZWFk
bnEyMDE5LmNybDAdBgNVHQ4EFgQU57/MeDSPd2GeTF1hmca3WDMj8XQwDgYDVR0PAQH/BAQDAgeA
MA0GCSqGSIb3DQEBCwUAAIBAQBC7/QjZnUyl4RVZ5tBZdSb6r+CkGHzrNIFjcZ/+0akWnhckIYI1
tTDf8wY4WhxoTF3jHgGEggjIPAUbzAta5MUOrqlWBFgNHSGW3bqMCfcbmAgbEIfR8HJSTVVSaQha
0flclwBVCnAN5RrdU/4+qFP17Kmcc9DAtieMCPOZieSk7VivOyJlHZjgxN/pEnVWH+oiekjrilGUf
YkubpgntTmCxQHak2NyeTSSBAn3i+apLCB5lcBBDtWiRKCHtRINU7nMkqLAtqmLcgZHB22po+4x1
rYg6vvQ8d8YsGJYPVRZXcHg69Po2thmgdc/Zh3EEF96rD1VIZa1Au2FqjLexvEE
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C:	*ES*
Issuer O:	*European Agency of Digital Trust, S.L.*
Issuer CN:	*EADTrust RSA 2048 SubCA For Non-Qualified Certificates 2019*
Subject C:	*ES*
Subject O:	*EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*
Subject 2.5.4.97:	*VATES-B85626240*
Subject OU:	*Entity Seal Certificate*
Subject CN:	*QTSU EPSILON EADTrust*
Valid from:	*Wed Nov 06 12:04:13 CET 2019*
Valid to:	*Sun Nov 05 12:04:13 CET 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D3:58:F8:8A:32:AF:34:6B:EF:68:D0:73:0C:19:14:6F:F9:55:03:30:49:D5:7F:C1:4D:37:75:AB:2A:AF:40:5E:9D:E2:B7:32:C4:F8:1E:7D:BE:D9:BF:3C:12:FC:A3:A3:1E:B5:04:A3:11:85:7F:24:59:B1:BB:50:C1:52:BE:1D:A8:9A:BC:8F:CD:7C:D3:BC:6F:AB:A2:80:E7:77:78:05:68:96:98:4F:C7:50:CD:73:0B:35:B7:37:AF:D7:B3:E6:D1:17:DA:D3:FD:7E:CF:25:F2:DE:A6:5E:EE:98:83:60:39:84:ED:49:7B:CB:7B:86:F6:5D:75:EC:50:A6:D6:C2:01:87:79:F1:04:BD:4D:0C:39:C0:F7:56:FC:3B:C4:7F:91:4D:9A:E5:6D:D8:80:3D:E6:33:9A:30:9E:63:83:55:D1:8F:F0:F4:75:7E:40:4B:5C:8C:7E:7C:32:DE:8F:1E:42:5D:A0:9A:BF:4B:FF:36:C4:AC:E1:33:7F:8B:92:A1:B3:01:5C:50:13:34:EB:13:2E:10:65:E6:85:21:E9:3C:78:09:E3:A8:3F:13:8A:45:16:C0:B3:81:C5:87:5D:CB:33:17:ED:A0:E3:14:D6:54:A0:D0:6A:53:4F:28:73:BC:F2:1B:93:D1:C5:99:D0:E5:32:62:EC:DD:D0:D8:CB:A7:02:03:01:00:01*
Authority Key Identifier	*E7:EB:E9:2F:72:EB:F9:59:BD:7D:50:E9:4E:18:D0:CF:28:59:17:22*
Authority Info Access	*http://ca.eadtrust.eu/eadtrust-subca-rsa2048eadnq2019.crt* *http://ocsp.eadtrust.eu*
Issuer Alternative Name	*ca@eadtrust.eu*
Subject Alternative Name	*ca@eadtrust.eu* *http://ca.eadtrust.eu* *http://www.eadtrust.eu* *http://policy.eadtrust.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.501.2.1.1.0.3161* *CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]* *CPS pointer: http://policy.eadtrust.eu*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://crl.eadtrust.eu/eadtrust-subca-rsa2048eadnq2019.crl*
Subject Key Identifier	*E7:BF:CC:78:34:8F:77:61:9E:4C:5D:61:99:C6:B7:58:33:23:F1:74*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *6B:61:40:20:33:60:08:6C:45:F0:73:77:B8:9C:51:35:C3:AB:5A:C2:C0:09:10:D9:20:1C:92:E8:DB:68:3F:61*

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Entity Seal Certificate*

Subject CN: *QTSU EPSILON EADTrust*

X509SKI

X509 SK I *57/MeDSPd2GeTF1hmca3WDMj8XQ=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

41 - TSP: Bewor tech, S.L.

.

TSP Name

Name	[en]	*Bewor tech, S.L.*
Name	[es]	*Bewor tech, S.L.*

TSP Trade Name

Name	[en]	*Bewor tech*
Name	[es]	*Bewor tech*
Name	[en]	*VATES-B19603968*
Name	[es]	*VATES-B19603968*

PostalAddress

Street Address	[en]	*P.I. Cortijo del Conde, Calle Pago de Cambea, 14 Nave 7*
Locality	[en]	*Granada*
State Or Province	[en]	*GRANADA*
Postal Code	[en]	*18015*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*P.I. Cortijo del Conde, Calle Pago de Cambea, 14 Nave*
Locality	[es]	*Granada*
State Or Province	[es]	*Granada*
Postal Code	[es]	*18015*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*http://bewor.com*
URI	[es]	*http://bewor.com*
URI	[en]	*mailto:info@bewor.com*

URI	*[es]*	*mailto:info@bewor.com*

TSP Information URI

URI	*[en]*	*http://www.bewor.com*
URI	*[es]*	*http://www.bewor.com*

41.1 - Service (granted): Qualified Certificates issued by BEWOR TECH CA1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by BEWOR TECH CA1*
Name	*[es]*	*Certificados cualificados emitidos por BEWOR TECH CA1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *4955006823150501412*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIILjCCBg6gAwIBAgIIRMO4c/GFvsQwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXUjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LnVbbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5B1jEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRswGQYDVQQDDBJVQUSBVEFDQSBST09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAe
Fw0yMDA1MTIwODQ2MzVaFw0zMzA1MTIwODQ2MzVaMHAxCzAJBgNVBAYTAkVTMRAwDgYDVQQHDAdH
UkFOQURBMRYwFAYDVQQKDA1CZXAdveiB0ZWNoIFNMMRIwEAYDVQQLDAlQU0MtQkVXT1IxFzAVBgNV
BAMMDkJFV09SIFRFQ0ggQ0ExMRgwFgYDVQRhDA9WQVRFUy1CMTk2MDM5NjgwggIiMA0GCSqGSIb3
DQEBAQUAA4ICDwAwggIKAoICAQCcU96W4lxIvCNJ/xtLzo8zk+FGpFS0Om7RTrmduuy0Ca7pRhTq
H8KxpNkI3V4v8TwHfZ25Nbg2Yg2RzfSdlPTd0WZiM+vJdMFxgn+2h2kwKc6yoc9tC2wXQpUMK
Ly/42AwmFaSSIo7yfIb1Ii61ysWQ/S1ul+U6NKEmEjAZcrJeIxT3Tpe+xcSMLJy/dY9/lAuLO9fP
LO4Jgvy3fntysh5kZoHk72KGtm78Q9zIIF7pFetaLwemJGy76n6CbeQ51cDdzSoINcXK5SxQ0b7V
KWiDBwQmzV5uX5gqEYnWIYn+9v+Gujd9ssSZTrmxDbraTPyPolRH4dzhMphHxsweQx/KGQvpjsl
k5PlGcml+acaPMld45CWk53vDGgi5M1Ym+1Spft6aS4UDMyJIRO32hRf7EFb35h8INvYZnu+o8uo
9903sdrl0LqGm5XqBrFP4btg/AW5utflQm+qrquts3nMUxG7mki2QKlyp8U7+Ca517SXKYup4vri
Bhx963hkkZoIV4FbK5bNyAdLIa0hDAH6BCl9uhl0fbKAOjCaMzLbWzCUz/6R8rOkDUkJgIj726YYD
WxdgMK/XU3csKeYGjF+PLPkX0wYnpPmpTlmuL+tdx7Dl40QUZAyIZzGqUlbkGKqiC92R90IR7Ek3g
aXOHFsovV38eMSUTctiXDSrO8t0IDAQABo4ICqjCCAmYwfgYIKwYBBQUHAQEEcjBwMDYGCCsGAQUF
BzABhipodHRwOi8vb2NzcDEudWFuYXRhY2EuY29tL3B1YimxpYy9wa2kvb2NzcC8wNgYIKwYBBQUH
MAGGKmh0dHA6Ly9vY3NwMi51YWShdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAdBgNVHQ4EFgQU
NgJawWS0+SnxAwkWILPZpr16E0lwEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBRVLPG8
oV657qAxiFcQW/yW95GaLDJkxBgNVHRIEFTATgBFpbmZxQHVhbmF0YWNlLmNvbTCBuAYDVR0gBIGw
MIGtMIGqBgRVHSAAMIGhMCEGCCsGAQUFBwIBFhVodHRwczovL2Jld29yLmNvbS9kcGMwIAYIKwYB
BQUHAgIwcAxuQ2VydGlmaWNhZG8gZGUgbGEgQXV0b3JpZGFkIGRlIENlcnRpZmlj YWNpw7NuIFN1
Ym9yZGluYWRhIGRlIEJld29yIHR1Y2ggLSBodHRwczovL2Jld29yLmNvbS9wcm92ZWVkb3lZGUt
ZmlybWEwgYsGA1UdHwSBgzCBgDA+oDygOoY4aHR0cDovL2NybDEudWFuYXRhY2EuY29tL3B1Ymxp
Yy9wa2kvY3lsL2FybF9lYW5hdGFjYS5jcmwwPqA8oDqGOGh0dHA6Ly9cmwyLnVhbmF0YWNlLmNv
bS9wdWJsaWMvcGtpL2NybC9hcmxfdWFuYXRhY2EuY3JsMA4GA1UdDwEB/wQEAwIBBjAZBgNVHREE
EjAQgQ5pbmZvQGJld29yLmNvbTANBgkqhkiG9w0BAQsFAAOCAgEAZfzITgBy4dje3zQzGf02IyQG
K56HjQm39fADpFm3gZz5RtGD0wZqnhkRUj3By22FTDrekaTxzpMOrC0tATu6TgOHFeHdEiJlpbKru
BbVd6oVA/7CB0Bkz4yIMAaJeUbudyVGIJMeHiTvIynrWUGucfyVAA6fb2DEYRUTtu3SSk0b8QCGl
xRY3nazyjbLBmCMt8eGpPlMCrAxnU1vR011q1bMa0mn6QedlKCYkg11nEKJnKNZsTjtPSzdyWupt
JV1z5mrJL1RZB1djywSElZlCCg/m/ncojb0uytRflK22jG0o61CFcnVCjxQB3AtIlewkEw+f224sO
qw/5JgN61RpVkrwmPUSVkVaMOAdDFPBtFg9cVTiLImUvONSakNf0L Hggs/N41zu/7MOD8dX09meK
UwgQk27YkX+swXMLuKUXrb6zw3FDTh27lLX8hLmNbAcPSTBP+kDMqq3wKXMlF1sQtq/cR9QG56M
EHrM6BFSRGCLkr1bHcRUMKrMIeV4wtNlgJ0TBpj8+2vaQwWnDt39klNgDlB//kFeR7YR7LPDQrU/u
NmTTeM1zo4Qjy9fdgqcC2qE1ZSOLAqU/01e8ie9VDw86qX9a5rPd041UWKiz5USQCwnake22ZNku2
Mm1C/Zhj1kPXsTRxMkjc9JD0d47oIAgfjWyElKgiFbawhb9qR24=

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA256withRSA*
Issuer 2.5.4.97:	*VATES-A66721499*
Issuer CN:	*UANATACA ROOT 2016*
Issuer OU:	*TSP-UANATACA*

Issuer O:	*UANATACA S.A.*
Issuer L:	*Barcelona (see current address at www.uanataca.com/address)*
Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-B19603968*
Subject CN:	*BEWOR TECH CA1*
Subject OU:	*PSC-BEWOR*
Subject O:	*Bewor tech SL*
Subject L:	*GRANADA*
Subject C:	*ES*
Valid from:	*Tue May 12 10:46:35 CEST 2020*
Valid to:	*Thu May 12 10:46:35 CEST 2033*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:53:DE:96:E2:5C:48:BC:23:49:FF:1B:4B:CE:8F:33:93:E1:46:A4:54:B4:3A:6E:D1:4E:B9:9D:BA:EC:B4:09:AE:E9:46:14:EA:25:F7:D1:C6:33:62:92:5D:D5:E2:FF:13:C0:57:DF:67:6E:4D:6E:0D:98:83:64:73:7D:27:65:3D:37:74:59:98:8C:FA:F2:5D:30:5C:60:9F:ED:A1:DA:4C:0A:73:AC:A8:73:D9:C2:DB:05:D0:A5:43:0A:2F:2F:F8:D8:0C:26:15:A4:B9:22:8E:F2:7C:86:F5:22:2E:B5:CA:C5:90:FD:2D:6E:97:E5:3A:34:A1:26:12:30:19:72:B2:5E:27:14:F7:4E:97:BE:C5:C4:8C:2C:9C:BF:75:8F:7F:94:0B:8B:3B:D7:CF:2C:EE:09:82:FC:B7:7E:7B:72:B2:1E:64:66:81:E4:EF:62:86:B6:6E:FC:43:DC:C8:20:5E:E9:15:EB:5A:2F:07:A6:24:6C:BB:EA:7E:82:6D:E4:39:D5:C0:DD:CD:2A:08:35:E5:CA:E5:2C:50:D1:BE:D5:29:68:83:07:04:26:CD:5E:6E:5F:98:2A:11:89:D6:95:89:FE:F6:FF:86:BA:37:7D:B2:C4:99:4E:B9:B1:0D:BA:DA:4C:FC:8F:A2:54:47:E1:DC:E1:32:98:47:C6:2B:30:79:0C:7F:28:64:2F:A6:3B:25:93:93:C9:19:C9:88:F9:A7:1A:3C:C9:5D:E3:90:96:93:9D:EF:0C:68:25:E4:CD:58:9B:ED:52:A5:FB:7A:69:2E:14:0C:CC:89:21:13:B7:DA:14:45:EC:41:5B:DF:96:D1:94:DB:D8:65:BC:3E:A3:CB:A8:F7:DD:37:B1:DA:E5:D0:BA:86:9B:95:EA:06:B1:4F:E1:BB:60:FC:05:B9:BA:D7:C8:42:6F:AA:AE:AB:AD:B3:79:CC:53:11:BB:9A:48:B6:40:A9:72:A7:C5:3B:F8:26:B9:D7:B4:97:29:8B:A9:E2:FA:E2:06:1C:7D:EB:78:64:91:9A:08:57:81:5B:2B:96:CD:C8:07:4B:95:AD:21:0C:01:FA:04:29:7D:BA:12:34:7D:B2:80:3A:30:9A:33:32:DB:5B:30:94:CC:9E:BC:AC:E9:03:52:42:60:22:3E:F6:E9:86:03:5B:17:60:30:AF:D7:53:77:2C:29:E6:06:8C:5F:8F:2C:F9:17:D3:06:27:A4:F9:A9:4C:89:AE:2F:EB:5D:C7:B0:C8:E3:44:14:64:0C:A5:67:31:AA:51:B9:06:2A:A8:82:F7:64:7D:D0:94:7B:12:4D:E0:69:73:81:16:CA:2F:57:7D:1E:31:25:13:72:DB:57:0D:2C:CE:6D:02:03:01:00:01*
Authority Info Access	*http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*36:02:5A:C1:64:B4:F9:29:F1:03:09:16:94:B3:D9:A6:BD:7A:13:42*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*
Issuer Alternative Name	*info@uanataca.com*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://bewor.com/dpc* *CPS text: [Certificado de la Autoridad de Certificación Subordinada de Bewor tech - https://bewor.com/proveedor-de-firma]*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl* *http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl*
Subject Alternative Name	*info@bewor.com*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *8A:38:6E:D1:C0:93:26:03:D3:B5:F4:78:9B:7F:CB:33:CF:09:C8:1A:56:DE:97:FC:82:67:47:95:6C:2E:78:6D*

X509SubjectName

Subject 2.5.4.97: *VATES-B19603968*

Subject CN: *BEWOR TECH CA1*

Subject OU: *PSC-BEWOR*

Subject O: *Bewor tech SL*

Subject L: *GRANADA*

Subject C: *ES*

X509SKI

X509 SK I *NgJawWS0+SnxAwkWlLPZpr16E0I=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-10-23T02:00:00Z

41.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

42 - TSP: ELECTRONIC IDENTIFICATION, S.L.

.

TSP Name

Name	*[en]*	*ELECTRONIC IDENTIFICATION, S.L.*
Name	*[es]*	*ELECTRONIC IDENTIFICATION, S.L.*

TSP Trade Name

Name	*[en]*	*Electronic Identification S.L.*
Name	*[es]*	*Electronic Identification S.L.*
Name	*[en]*	*VATES-B86681533*

PostalAddress

Street Address	*[en]*	*Avenida Ciudad de Barcelona, 81. 4ª Planta.*
Locality	*[en]*	*Madrid*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28004*
Country Name	*[en]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:ivan@electronicid.eu*
URI	*[en]*	*https://www.electronicid.eu*

TSP Information URI

URI	*[en]*	*https://www.electronicid.eu*

42.1 - Service (granted): Qualified Certificates issued by ELECTRONIC IDENTIFICATION CA1

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by ELECTRONIC IDENTIFICATION CA1*

Name *[es]* *Certificados Reconocidos emitidos por ELECTRONIC IDENTIFICATION CA1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3945188695639549777*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIldTCCBl2gAwIBAgIINsAgN1d7Z1EwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRswGQYDVQQDDBJVQUSBVEFDQSBST09UIDIwMTYxGDAWBgNVBGEMDUZBVEVTLUE2NjcyMTQ5OTAe
FwI0yMDAyMjUxMDU3MTNaFw0zMzAyMjQxMDU3MTNaMIGbMQ8wCQYDVQQGEwJFUzEPMA0GA1UEBwwG
TUFEUkIEMScwJQYDVQQKDB5FbGVjdHUvbmljIElkZW50aWZpY2F0aW9uIFMuTC4xEDAOBgNVBAsM
B1BTQy1FSUQxJjAkBgNVBAMMHUVMRUNUUk9SUMgSURFTIRJRkIDQVRJT04gQ0ExMRgwFgYDVQRh
DA9WQVRFUy1CODY2ODE1MzMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDAFOTSwnEB
JSAM6bt9fT5ETiVHAtI1K88SqGC6Rd+5tUMhUmHUck5m1PZxJzUsMUNndPBfiRIi2os4upOmvrwNs
k0bOifdTKh6qwmN5UqstbL9QH2W3eL YcUZHH11dY/be3PZSUICrMZZRUT/YP5GBhhJR+uy69AYJ8V
zeLwjMtlguse840QBRALuPRP7Q4U2P//hfFvw2vlZAEpnAFeO4pK6Ey9dzXciZpPteL/9CYf1Cl4
8fNpFs85Pjsl/2xKycrR1Yc0dCTe6yCTlzFPbZX5xsKicMzvFdsN//6BFckb/1f8bW7ywZkgBHUf
uvNkLrL7LfDdvYdGMbvzfS5Ozz7j+nXFs1MYc0qs4fumynhptmpkR1n/+JDMNf3uTFWfXUZO9dy4
cfr7azLm+Y+a+6ARud8K8aKRCHUFqOEMWKJB4T7C1a1+/omPvXcAHjB8nt1Eqw4tACQQbbB3AHbd
d5bnwp4mxu/o97kvfI0TCE5c+IqaeLZWW8SXDmRHv2hQTkCA1Gtc5qJLnC/M0aWbyd0XFkYj9Xjz
oa4k0oYSRf+0wbKrhTlYQu8t14dLvOxuufRlOx1ZZfQwVEqPvIJjN8t5K97POJZkyao0cFG5iwAo
06bvLfxEgq7kDU05OZ0UxZatSQ7SUB9f9kA9bfkeg+9RQBSNUdj7BCossJmaOQ0wIDAQAHo4IC
mzCCApcwfgYIKwYBBQUHAQEEcjBwMDYGCCsGAQUFBzABhipodHRwOi8vb2NzcDEudWFuYXRhY2Eu
Y29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUHMAGGKmh0dHA6Ly9vY3NwMi51YWShdGFjYS5j
b20vcHVibGljL3BraS9vY3NwLzAdBgNVHQ4EFgQUbRVkzZsHSJ335ppEB5x5Coyhhj8wEgYDVR0T
AQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBRVLPG8oV657qAvrFcQWy/W95GaLIDAcBgNVHRIEFTAT
gRFpbmZvQHVhbmF0YWNhLmNvbTCB4wYDVR0gBIHbMIHYMIHVBgRVHSAAMIHHMME0GCCsGAQUFBwIB
FkFodHRwczovL3d3dy5lbGVjdHUvbmljaWQuZXUvY2VydGlmaWNhdGlvbi1wcmFjdGljZS1zdGF0
ZW1lbnQtY3BkLzB7BggrBgEFBQcCAjBvDG1DZXJ0aWZpY2FkbyBkZSBsYSBBdXRvcmlkYWQgZGUg
Q2VydGlmaWNhY2nDs24gU3Vib3JkaW5hZGEgZGUgRWxlY3Ryb25pYyBJRGVudGlmaWNhdGlvbs4g
LSB3d5euZWxlY3Rvb25pYZlkLmV1MiGLBgNVHR8EgYMwgYAwPqA8oDqGGhfdHA6Ly9zcmwxLnVh
bmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9hcmxfdWFuYXRhY2EuY3JsMD6gPKA6hjhodHRwOi8v
Y3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvYXJsX3VhbmF0YWNhLmNvbDAOBgNVHQ8B
Af8EBAMCAQYwHwYDVR0RBBgwFoEUaW5mb0BlbGVjdHUvbmljaWQuZXUwDQYJKoZIhvcNAQELBQAD
ggIBAHzOsbL1Ip7Saspnn9DWYMtuT79NC/02h0h8P1PZR0zz3KAkdrO4G1hg92vKqzhjgJsHMYt2
zV8XYQ487T2S/pKbIMTTDFHRwSNyU5S4z8p4gufCF8kkrZlRim0SKBtiaYnKLqmtyiLjnPvegwp
q3gVcg8afKI5qxnShchNH+IvcNx/QC7MePku0FAZY9naFEPmcdSs3mGiVHZbuv5eWsqm4/BMx+4X
PBmHO8Vij2iHzUdfCavkXkocDA8+7WB+aQHZ3gHZQvC0pFKSwO6YSdo8d/IfCzUJ7yADUkVvDW4
DMoax6wnXc8b9WQkjWHPXSHLMs9JkzLtE3Lws9C/1UMbf4a7U4wkt55M3nYO2nt7AEwS9oKSDr
3hQsN6IA/IMwoYj4oMLJ9U6ytcYTNUQlNRWShyLdfWMwtOZmhlQXbbYqlXHhwVqL1hjlQ6bPOARKO
o186ol5cP0LEV4chDDVQoHZFgRjeMPD/UEOp83v9Q4swHZjzTlsBhlRhZH5g+TWXTYBPOs94quaJ
RI9QVlVk7lCEsQA611F1XG4tkX7CuvaOdPjvlVBrJPM4oREsU1YXxNzew3+NH1IJ4SS/Rpwiwctl/
pepRvRyrQlKf4bHqMTXh04CsE19/ESRLjxy7VnCD1TbrYo7TCAoOQMbQwK9nEOIOOeTs2d3QXqGqK
XRth

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA ROOT 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B86681533*

Subject CN: *ELECTRONIC IDENTIFICATION CA1*

Subject OU: *PSC-EID*

Subject O: *Electronic Identification S.L.*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Tue Feb 25 11:57:13 CET 2020*

Valid to: *Thu Feb 24 11:57:13 CET 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C0:14:E4:D2:C2:71:01:25:20:0C:EA:1F:45:4F:91:13:89:51:C0:B4:8D:4A:F3:CE:6A:18:2E:81:77:EE:62:50:C8:54:98:75:1E:93:99:B5:3D:9C:49:CD:4B:0C:50:D9:DD:3C:17:DA:44:88:B6:A2:CE:2E:A4:E9:F0:AF:03:6C:93:46:CE:7D:D4:CA:87:AA:B0:98:DE:54:AA:CB:5B:2F:D4:07:D9:6D:DE:2D:87:94:64:71:F5:D5:D6:3F:6D:ED:CF:65:25:08:0A:B3:19:65:15:13:FD:83:F9:18:18:61:25:1F:AE:CB:AF:40:60:9F:15:CD:E2:F0:8C:CB:65:82:EB:1E:F3:8D:10:05:10:0B:B8:F4:4F:ED:0E:14:D8:FF:FF:85:F1:6F:C3:6B:E5:64:01:29:9C:01:5E:3B:8A:4A:E8:4C:BD:77:35:DC:89:9A:4F:B5:E2:FF:F4:26:1F:D4:29:78:F1:F3:69:16:CF:39:3E:3B:25:FF:6C:4A:C9:CA:D1:21:87:34:74:24:DE:EB:20:93:97:31:4F:6D:95:F9:C6:C2:A2:70:CC:EF:15:DB:0D:FF:FE:81:15:C9:1B:FF:57:FC:85:6E:F2:C1:99:20:04:75:1F:BA:F3:64:2E:B2:FB:2D:F0:DD:BD:87:46:33:CB:F3:7D:2E:4E:CF:3E:E3:FA:75:C5:B3:53:18:73:48:38:88:8B:A6:CA:78:69:B6:6A:64:47:59:FF:F8:90:CC:35:FD:EE:4C:55:A5:5D:46:4E:F5:DC:B8:71:FA:FB:CE:A2:E6:F9:8F:9A:FB:A0:11:B9:DF:0A:F1:A2:91:08:75:05:A8:E1:0C:58:A2:41:E1:3E:C2:D5:AD:7E:FE:B9:8F:BD:77:80:1E:30:7C:9E:DD:44:AB:0E:2D:00:24:10:85:B0:77:00:76:DD:77:96:E7:C2:9E:26:C6:EF:E8:F7:B9:2F:7C:8D:13:08:4E:5C:F8:8A:9A:70:B6:56:5B:C4:97:0E:64:47:BF:68:50:4E:40:80:D4:6B:5E:E6:A2:4B:9C:2F:CC:D1:A5:9B:C9:DD:17:16:46:23:F5:78:F3:A1:AE:24:D2:86:12:44:8F:B4:C1:B2:AB:85:39:58:42:EF:2D:D7:87:4B:BC:EC:6E:8D:F4:65:3B:1D:59:65:F4:30:54:4A:8F:BC:82:63:37:CB:79:2B:DE:CF:38:8D:A4:C9:AA:0E:70:51:B9:8B:00:28:D3:A6:EF:2D:FC:44:82:AE:E4:0D:4D:39:39:9D:14:C5:9B:AD:E5:0E:D2:50:1F:5F:F6:59:00:F5:B1:64:7A:0F:BD:45:0B:41:48:D5:1D:8F:B0:42:A2:CB:C9:99:A3:90:D3:02:03:01:00:01

Authority Info Access

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *85:15:64:CD:9B:07:48:9D:F7:E6:9A:44:07:9C:79:0A:8C:A1:96:3F*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.electronicid.eu/certification-practice-statement-cpd/

CPS text: [Certificado de la Autoridad de Certificación Subordinada de Electronic IDentification. - www.electronicid.eu]

CRL Distribution Points

http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl

http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

Subject Alternative Name *info@electronicid.eu*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EE:DC:F3:16:33:60:9A:CB:49:28:95:FD:55:AA:59:1A:10:9C:44:D3:B0:FC:1D:06:21:E0:FB:41:A2:CB:49:2B*

X509SubjectName

Subject 2.5.4.97: *VATES-B86681533*

Subject CN: *ELECTRONIC IDENTIFICATION CA1*

Subject OU: *PSC-EID*

Subject O: *Electronic Identification S.L.*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *hRVkzZsHSJ335ppEB5x5Coyhlj8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2020-11-18T22:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

URI *[es]* *https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx*

42.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

42.1.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.55193.1.1.2*

Description

43 - TSP: Sectigo (Europe) SL

.

TSP Name

Name	[en]	Sectigo (Europe) SL
Name	[es]	Sectigo (Europe) SL

TSP Trade Name

Name	[en]	SECTIGO
Name	[es]	SECTIGO
Name	[en]	VATES-B01683580

PostalAddress

Street Address	[en]	Rambla Catalunya 86, 3º1
Locality	[en]	Barcelona
State Or Province	[en]	Barceona
Postal Code	[en]	08008
Country Name	[en]	ES

ElectronicAddress

URI	[en]	https://www.sectigo.com
URI	[en]	mailto:inigo.barreira@sectigo.com

TSP Information URI

URI	[en]	https://www.sectigo.com

43.1 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Website Authentication CA E35”

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	*[en]*	*Qualified Certificates issued by “Sectigo Qualified Website Authentication CA E35”*
Name	*[es]*	*Certificados cualificados emitidos por “Sectigo Qualified Website Authentication CA E35”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *210467423367101675439552997939815733505*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIDbjCCAvSgAwIBAgIRAJ5WjSHc2JMHw0CA/v2ZWQEwCgYIKoZIzj0EAwMwgYgxCzAJBgNVBAYT
AlVTMRMwEQYDVQQIEwpOZXcgSmVyc2V5MRQwEgYDVQQHEwtKZXJzZXlgQ2l0eTEeMBwGA1UEChMV
VGhlIFVTRVJUUlVTVCBOZXR3b3JrMS4wLAYDVQQDEyVVU0VSVHJ1c3QgRUNDIENlcnRpZmlfYXRp
b24gQXV0aG9yaXR5MB4XDTIwMTAwNTAwMDAwMFoXDTM1MTAwNDEzNTk1OVowZTELMAkGA1UEBhMC
RVMxHDAaBgNVBAoTE1NlY3RpZ28gKEV1cm9wZSkgU0wxODA2BgNVBAMTL1NlY3RpZ28gUXVhbGlm
aWVkIFdlYnNpdGUgQXV0aGVudGlj YXRpb24gQ0EgRTM1MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcD
QgAEoZ/maiXB18YoY6slFi0kuyZTQltgwxwjnljRZ8u/VLF3L4b1NgZAlNTwGR1QLIYgGOBZx2k8
cSr+E4wS3gARlaOCAV8wggFbMB8GA1UdIwQYMBaAFDrhCYbUzxatCInZ0SXbc4DXGY2OaMB0GA1Ud
DgQWBBQBEL B9TETSoLJg+cqafitaKr56vWTAOBgNVHQ8BAf8EBAMCAYYwEgYDVR0TAQH/BAgwBgEB
/wIBADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEQYDVR0gBAowCDAGBgRVHSAAMFAG
A1UdHwRJMEcwRaBDoEGGP2h0dHA6Ly9jcmwudXNlcnRydXN0LmNvbS9VU0VSVHJ1c3RFQ0NDZXJ0
aWZpY2F0aW9uQXV0aG9yaXR5LmNybDBxBggrBgEFBQcBAQRlMGMwOgYIKwYBBQUHMAKGLmh0dHA6
Ly9cmQudXNlcnRydXN0LmNvbS9VU0VSVHJ1c3RFQ0NBQUFDQS5jcmQwJQYIKwYBBQUHMAGGGWh0
dHA6Ly9vY3NwLnVzZXJ0cnVzdC5jb20wCgYIKoZIzj0EAwMDaAAwZQIxAPdGdzU3wUj6nUMuGR88
wpKNe8anlEp+ilkEqq9E4Trb/Vsl+0Kza3bZxD1+TpLX1wIwSn26MmiP43/g/EVOPLSG/jw9EEod
K6gdSA8irkWi7SmhFPLMduOCbAGR7MVbVBV

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer CN: *USERTrust ECC Certification Authority*

Issuer O: *The USERTRUST Network*

Issuer L: *Jersey City*

Issuer ST: *New Jersey*

Issuer C: *US*

Subject CN: *Sectigo Qualified Website Authentication CA E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Mon Oct 05 02:00:00 CEST 2020*

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key:

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:A1:9F:E6:6A:25:C1:D7:C6:28:63:AB:08:16:2D:24:BB:26:53:42:5B:60:C3:1C:23:9E:58:D1:67:CB:BF:54:B1:77:2F:86:F5:36:06:40:94:D4:F0:19:1D:50:2C:86:20:18:E0:59:C7:69:3C:73:CA:FE:13:8C:12:DE:00:11:95

Authority Key Identifier *3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A*

Subject Key Identifier *01:10:B0:7D:4C:44:D2:A0:B2:60:F9:E8:DA:7D:FB:8A:AF:9E:AF:59*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_serverAuth*

Certificate Policies	*Policy OID: 2.5.29.32.0*
CRL Distribution Points	*http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl*
Authority Info Access	*http://crt.usertrust.com/USERTrustECCAAACA.crt* *http://ocsp.usertrust.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*56:2D:6A:5B:4B:06:74:65:FF:D0:FB:FC:9B:B0:57:55:CD:AC:F5:5B:5E:E5:C6:F9:10:B8:B5:3D:B1:28:F5:7A*

X509SubjectName

Subject CN:	*Sectigo Qualified Website Authentication CA E35*
Subject O:	*Sectigo (Europe) SL*
Subject C:	*ES*

X509SKI

X509 SK I	*ARCwfUxE0qCyYPno2n37iq+er1k=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-05-05T01:00:00Z

43.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

43.2 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Website Authentication CA R35”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by “Sectigo Qualified Website Authentication CA R35”*

Name *[es]* *Certificados cualificados emitidos por “Sectigo Qualified Website Authentication CA R35”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *523498626239595397042119236715994076 48*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGWTCCBEGgAwIBAgIQJ2I3gEihs2KNUH4pIg3ilDANBgkqhkiG9w0BAQwFADCBiDELMAkGA1UE
BhMCVVMxEzARBgNVBAgTCKSldyBKZXJzZXkxFDASBgNVBAcTC0plcnNleSBDaXR5MR4wHAYDVQQK
ExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNVBAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwHhcNMjAxMDA1MDAwMDAwWhcNMzUxMDA0MjM1OTU5WjBlMQswCQYDVQQG
EwJfUzEcMBoGA1UEChMTU2VjdGlnbyAoRXVyb3BlKSBTTDE4MDYGA1UEAxMvU2VjdGlnbyBRdWFs
aWZpZWQgV2Vic2l0ZSBBdXRoZW50aWNhdGlvbiBDQSBSMzUwggGMA0GCSqGSIb3DQEBAQUAA4IB
jwAwggGKAoIBgQDM22r2ErDUlj/ol7CQ6ex30UeqGqLXS9PBwLUcE7mjg7BLPEcXb1axVekRweC5
lxEXSfrzTc5lqsk+idax7butIvU7TBP8YWxEPeZPy/wM07LEY4I51c/dJNBokyjJZttCejrQjY
tHPaYsCP6NplHxmupjZoOKyFHIAtBzrY3Mb77tEjpP4gvxEC7OtBdV+AFQp4XBxlc29S4ttUs6lDbV
c6NsjEgEWEnNMpQp07MuwjDCypQrEtKaepo/iGUWwkecV662K8mifLTDRSDf+kF3m+kWZe2eylEP
zH9hnOOG7LF0ivpmjujwUJP0zs96KH98yWp1jDJdP1Y/k2h6tVPjV+RV/qd7HKr8E2RWwT+HvX+3
OHjdn8B20+M2lEVsR7cJpTtcWznYGmsDZm6bZ46o0kbVIFIL TDBRLH64lIQcsYObED5bjMUfqYaoL1
PZI2DvFTBdDLu2K6tYsgjonbtGM+Z05sDYtRZN9Mkc14QPmNnMFvEbckY/h7bSZPZqDdPmrWECAwEA
AaOCA V8wggFbMB8GA1UdIwQYMBaAFFN5v1qqK0rPVIDh2jvAnfKyA2bLMB0GA1UdDgQWBBTrNSUq
Bjbo1gHlaZOE0vMsO6zerzAOBgNVHQ8BAf8EBAMCAYYwEgYDVR0TAQH/BAgwBgEB/wIBADAdBgNV
HSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEQYDVR0gBAonCTDAGBgRVHSAAMFAGA1UdHwRJMEcw
RtBDoEGGP2hldHA6L y9jcmwudXNlcnRydXN0LmNvbS9VU0VSVHJ1c3RSU0FDZXJ0aWZpY2F0aW9u
QXV0aG9yaXR5LmNybDBxBggrBgEFBQcBAQRlMGMwOgYIKwYBBQUHMAKGLmhtdHA6Ly9jcnQudXNl
cnRydXN0LmNvbS9VU0VSVHJ1c3RSU0FBQUFDQS5jcnQwJQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3Nw
LnVzZXJ0cnVzdC5jb20wDQYJKoZIhvcNAQEMBQADggIBAGBpLCrwnPEtnVgL81NkkYCZmvWOvc1
vPPkia7EJALzPqnd+4E0/xMhkgY0zMz6YOxZYRM35Q1R2b4KQ+UnK7OZu6anT1sudlwAa8r56Y3U
pTZda6mQcyCn6rBdYWHbE5QkSQmVa6cMIrQGK/N6AIl3oKLU83R+vwDdbUqnEiIPwsf2Iqxjon
mhox+MSCQVD303cPMNxwDIznQrAfQF5swgYepHQqXBihDraIYHQmrU2kLSLVMPFsx2FY936YypA6
Wht8OtC30NsZcp8cc31JoaIJHC9PYuU7rJqEBLR30sYuc7RrPILvcCAHjV5eVnV+yyyFg0Sy+zD
Hs7kEkBRXIrv/AaHXKaZ87YugRyGWk3vd4w6ogGilUtMn673/5DbeeDmReXhHjZnfCd2v2eOGI8G
YuEAlu6ppbQfz+vDb+CQsCeMs+QS31jLveOsnf83bAE8JU3rWFIIB31pc2ecVerffb/8PfC1cSY
GE/y8YxqJBlkjZ2d4NV1kPOEYE332NnkGi0K3+LInbbun/Qg/OasbYdwCIl89G6fK/XhbklEO/Da
2WbWbDzLuEOgXvTi01H8T5qAP6XY+ShBHmysuv36J6bkDHlkxC iyNB7PEzLMswjjSYsb3V6WCDop
z9jbhfiXzDy+Tu/QO5y4nlWplvX/ZdOM6NMmf1pYg12r

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer CN: *USERTrust RSA Certification Authority*

Issuer O: *The USERTRUST Network*

Issuer L: *Jersey City*

Issuer ST: *New Jersey*

Issuer C: *US*

Subject CN: *Sectigo Qualified Website Authentication CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Mon Oct 05 02:00:00 CEST 2020*

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:CC:DB:6A:F6:12:B0:D4:96:3F:E8:23:B0:90:E9:EC:77:D1:47:AA:1A:A2:D7:4B:D3:C1:C0:B5:1C:13:B9:A3:83:B0:4
B:3C:47:17:6F:56:B1:55:E9:11:C1:E0:B9:23:11:17:B0:9A:F3:AD:37:39:26:AB:24:FA:27:5A:C7:B6:EE:B4:8B:D4:ED:30:4F:F1:85:B1:10:F7:19:3E:3F:F0:33:4E:CB:11:8E:08:E7:57:3F:74:93:41:A2:4C:A3:25:9B:6D:09:E8:E
B:43:F8:D8:7C:73:DA:62:C0:8F:E8:DA:47:C6:7B:A9:8D:9A:0E:2B:21:47:20:00:71:AE:26:37:31:BE:FB:AC:4A:4F:E2:0B:F1:10:2E:CE:B4:17:55:F8:01:50:A7:85:C1:C4:87:36:F7:9E:34:B5:4B:3A:94:36:D5:73:A3:6C:8C:48
:04:58:49:CD:32:94:29:D3:B3:2E:C2:30:C2:CA:94:2B:12:D2:9A:7A:9A:3F:88:65:16:C2:47:9C:57:AE:B6:2B:C9:A2:7C:B4:C3:45:20:DF:FA:41:77:9B:E9:16:65:ED:9E:CA:51:0F:CC:7F:61:9C:E3:86:EC:B1:74:8A:FA:66:8E
:E8:F0:50:93:F4:CE:CF:7A:28:7F:7C:C9:6A:75:8C:32:5D:3F:56:3F:93:68:7A:B5:53:E3:57:E4:55:FE:A7:7B:1C:AA:FC:13:64:56:C1:3F:87:BD:7F:B7:38:78:DD:9F:C0:76:D3:E3:36:24:45:6C:47:B7:09:A5:3B:5C:5B:39:D8:1
A:6E:19:99:B6:78:EA:8D:24:6D:52:05:20:B4:C3:05:12:C7:EB:82:08:41:CB:18:39:B1:03:E6:18:CC:25:FA:98:6A:82:C8:3D:92:36:0E:F1:41:74:32:E7:D8:AE:A2:62:C8:23:A3:06:C6:33:E6:4E:E5:D0:D8:B5:16:4D:F4:C9:1E:
D7:84:0F:98:D9:CC:16:F1:21:72:46:3F:87:B8:79:64:FD:AA:0D:D3:EE:B9:61:02:03:01:00:01

Authority Key Identifier *53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB*

Subject Key Identifier *EB:35:25:2A:06:36:E8:D6:01:E5:69:93:84:D2:F3:2C:3B:AC:DE:AF*

Basic Constraints	*IsCA: true - Path length: 0*
Extended Key Usage	*id_kp_serverAuth*
Certificate Policies	*Policy OID: 2.5.29.32.0*
CRL Distribution Points	*http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl*
Authority Info Access	*http://crt.usertrust.com/USERTrustRSAAAACA.crt* *http://ocsp.usertrust.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*00:23:93:FA:0A:68:25:F7:7E:F6:86:E2:08:62:0B:97:17:77:91:F0:2F:07:DB:25:18:48:0F:BE:37:CE:7B:D8*

X509SubjectName

Subject CN:	*Sectigo Qualified Website Authentication CA R35*
Subject O:	*Sectigo (Europe) SL*
Subject C:	*ES*

X509SKI

X509 SK I	*6zUlKgY26NYB5WmThNLzLDus3q8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time *2021-05-05T01:00:00Z*

43.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

43.3 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Time Stamping CA R35”

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified Certificates issued by “Sectigo Qualified Time Stamping CA R35”*

Name *[es]* *Certificados cualificados emitidos por “Sectigo Qualified Time Stamping CA R35”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *170853138050611189885395079998180409 23*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGKDCCBBCgAwIBAgIQDNqDAdPzKA5szbAoo1LGWzANBgkqhkiG9w0BAQwFADBeMQswCQYDVQQG
EwJFTUzEcMBoGA1UEChMTUlZVjdGlnbyAoRXVyb3BlKSBTTDExMC8GA1UEAxMoU2VjdGlnbyBRdWFs
aWZpZWQgVGltZSBTdGFtcGluZyBSb290IFI0NTAeFw0yMDEwMDUwMDAwMDBaFw0zNTEwMDQyMzU5
NTlaMFwxCzAJBgNVBAYTAkVTMRwwGgYDVQQKExNTZWN0aWdvIChFdXJvcGUpIFNMMS8wLQYDVQQD
EyZTZWN0aWdvIFF1YWxpZmllZCBUaW1lIFN0YW1wa W5nIENBIFIzNTCCAaIwDQYJKoZIhvcNAQEB
BQADggGPADCCAYoCggGBAJGXuY4bMcH4zfMnKvsI8bc1YG1r8kMzKHGT1v/OUub4wrzLQPQtIwY
siWHPpg2m5MCzKSeukDGqas4qgUlF/6hubHo6TgF2QQtkREw2nQrV8PFTZIVE8lObaZCurwwn4lp
pJmUL1WoqLxHZClrvTSEUYlsF1ZVqDXe5jyKS4PBc83dLroEn6nuITBhE+z5DGCv97HV3UhMcIJM
uKTZmQrtiUjH0ozg3lnzVPI2T8y3A17APvWlbLmsf3waY54vIGq0rAdLLbbwPRUGWYHZU4W7nkgJ
ftiLQIfa+d0T/1FG4yPIXTWKTwmLZC6fDXUbfZSOcoP2c6C20g7Mo6jRlGPdYQJqVaIGajPrEUYu
iNJ+AuYQnMDMIwMqrv8BjygtElg/wm9lg1GBK4Z gbsZY4PYmZVkFTecockAsF0TdF7nsdMbTw5
Ta7fFyNDohdSq0jgB3L19X8SjTQYC99beCY1RPU3B9ZG02Zrl6yiPVORLbbULioWavwK56L0TLdD
ywIDAQABo4IBYjCCAV4wHwYDVR0jBBgwFoAUWYGow4Vk5+NEpGlSJpR79jsN7t4wHQYDVR0OBBYE
FGEAP3IZ+o50pGlHL6dNcd4XqRnMA4GA1UdDwEB/wQEAwIBhjASBgNVHRMBAf8ECDAGAQH/AgEA
MBMGA1UdJQQMMAoGCCsGAQUFBwMDMBEGA1UdIAQKMAgwBgYEVR0gADBPBgNVHRKESDBGMESgQqBA
hjSodHRwOi8vY3JsLnNlY3RpZ28uY29tL1NlY3RpZ28uY29tL1NlY3RpZ28RdWFsaWZpZWRUaW1lU3RhbXBpbmdSb290
UjQ1LmNybDB/BggrBgEFBQcBAQRzMHEwSgYIKwYBBQUHMAKGPmh0dHA6Ly9jcnQuc2VjdGlnby5j
b20vU2VjdGlnb1FlYWxpZmllZFRpbWVTdGFtcGluZ1Jvb3RSNDUuY3U0MCMGCCsGAQUFBzABhhdo
dHRwOi8vb2NzcC5zZWNlaWdvLmNvbTANBgkqhkiG9w0BAQwFAAOCAgEAGKD7dlD2eo2soxTBIqBk
THErw6HmVmrdjKjvyVzyKeU1V9GUzLKG5YwIx1zuSiU8Mg2vwb4MZmSI7278CBZAEnGyJ745e8z
dFmLb4N/I9HvYGh/4YHCWEGBOkJF2Viuctf4JszgyGgEixEKDqEN79sLy5HlUyEQbkXESbYePAPH
0IdioWor4wdWw4JvcWgt7N88KD7bpNZ2dfQCEEcL7tbcVtg06xdL 7Bq94ZzCEOeAS3tVfe1IvLM
jrIMOu2cjCXqK7Qa7qYzZF3FAkPozZdHKWYc22XQrtkvB6kBkIkdT7WGrtoLkNQezK4w8mVFS
Fx0V7b97nh1Q9VtOt0s/2AJshPOt0KBE0Z6FD88eN6pZ11J/1owa0x41+BPBhcQSG7jVt9VCml3s
aGiO787VADMzIldVr5wb9mGmO8mByW6VIRE+VAgyY7AYDLJxftzvjptVQPM63Hkilqxib7WfTAHq
LbSgEEZmJc2Hcit10i2q8xlgLD8ADWckMkbQVKjJul1RzTQsbOFHDTC+ZvuAthQ+7EnTInBsVXQO
lSqo7i6NWa6SAoDHoXsjPBr92xcmgMeO9kmf1kTKPgdNYLvCcOcXarvDLpRQbJkorzbEJULq6i53
cQsdTbeu5gPYoH+xUiuOGzTMPtZfi2IJJMGOPkAcLEwgZGkdIzf4i97U=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer CN: *Sectigo Qualified Time Stamping Root R45*

Issuer O: *Sectigo (Europe) SL*

Issuer C: *ES*

Subject CN: *Sectigo Qualified Time Stamping CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Mon Oct 05 02:00:00 CEST 2020*

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key:


```
30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:81:97:8E:E6:38:6C:C7:07:E3:37:CC:9C:AC:A2:23:C6:DC:D5:81:B5:AF:C9:0C:CC:A1:C6:15:4B:FF:39:4B:9B:E3:0
A:F3:2D:03:D0:B4:8C:1E:B2:25:87:3E:98:36:9B:93:02:CC:A4:9E:BA:40:C6:A9:AB:38:AA:05:25:17:FE:A1:B9:B1:FA:A1:38:05:D9:04:22:91:11:30:DA:74:2B:57:C3:C5:4D:92:15:13:C9:4E:6D:A6:42:BA:BC:30:9F:89:69:A
4:99:94:2F:55:A8:A8:BC:47:64:29:6B:BD:34:84:51:89:6C:17:56:55:A8:35:DE:E6:3C:8A:4B:83:C1:73:CD:DD:2E:BA:04:9F:A9:EE:21:30:61:13:EC:F9:0C:60:AF:F7:B1:D5:DD:48:4C:70:82:4C:B8:A4:D9:99:0A:ED:89:48:C
7:D2:8C:E0:DE:59:F3:54:F2:36:4F:CC:B7:03:5E:C0:3F:25:89:6C:B9:AC:7F:7C:1A:63:9E:2F:20:6A:B4:AC:07:4B:2D:B6:F0:3D:15:06:59:81:D9:53:85:BB:9E:48:09:7C:88:8B:40:87:DA:F9:DD:13:FF:51:46:E3:23:C9:5D:35:
8A:D7:09:CB:64:2E:A5:0D:75:1B:7D:94:8E:C6:83:F6:79:00:B6:D2:0E:CC:CF:A8:D1:94:63:DD:61:02:6A:55:A2:06:6A:33:EB:11:46:2E:88:D2:7E:02:E6:10:9C:C0:CC:22:DC:0C:AA:BB:FC:06:3C:A0:B4:49:60:FF:09:BD:9
6:0D:46:04:AE:09:DA:06:EC:65:8E:0F:62:66:55:90:54:DE:72:87:24:02:C1:74:4D:D7:FB:9E:C7:4C:6D:3C:39:4D:AE:DF:17:23:43:A2:17:52:AB:48:E0:07:72:F5:F5:7F:12:8D:34:18:0B:DF:5B:78:26:35:44:F5:37:07:D6:46:D
3:66:0B:97:AC:A2:3D:53:91:2D:B6:D4:2E:2A:16:6A:FC:0A:E7:A2:F4:4C:B7:43:CB:02:03:01:00:01
```


Authority Key Identifier *59:81:A8:C3:85:64:E7:E3:44:A4:69:52:26:94:53:F6:3B:0D:EE:DE*

Subject Key Identifier *61:00:3F:77:D9:FF:EA:39:D2:91:A5:1C:BE:9D:35:C7:78:5E:A4:67*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage	*id_kp_timeStamping*
Certificate Policies	*Policy OID: 2.5.29.32.0*
CRL Distribution Points	*http://crl.sectigo.com/SectigoQualifiedTimeStampingRootR45.crl*
Authority Info Access	*http://crt.sectigo.com/SectigoQualifiedTimeStampingRootR45.crt* *http://ocsp.sectigo.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*CD:0A:3E:00:A1:BD:AE:3A:15:9F:A9:E3:D7:0F:8E:66:4F:56:0F:DC:E1:63:57:CB:E4:40:ED:0B:0D:88:24:4F*

X509SubjectName

Subject CN:	*Sectigo Qualified Time Stamping CA R35*
Subject O:	*Sectigo (Europe) SL*
Subject C:	*ES*

X509SKI

X509 SK I	*YQA/d9n/6jnSkaUcvp01x3hepGc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*
	[es]	*undefined.*

Status Starting Time

2021-05-05T01:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://avancedigital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_en.aspx*

43.4 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Natural Person CA E35”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[es]	*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	*[en]*	*Qualified Certificates issued by “Sectigo Qualified Natural Person CA E35”*

Name *[es]* *Certificados cualificados emitidos por "Sectigo Qualified Natural Person CA E35"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *255804324125549905159335600213648333605*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDSzCCAtKgAwIBAgIRAMByHusGrZsheA+k20jJ2yUwCgYIKoZIzj0EAwMwXzELMAkGA1UEBhMC
RVMxHDAaBgNVBAoTE1NlY3RpZ28gKEV1cm9wZSkgU0wxMjAwBgNVBAMTKVNlY3RpZ28gUXVhbGlm
aWVkIEShdHVyYWwgUGVyc29uIFJvb3QgRTQ1MB4XDTIwMTAwNTAwMDAwMFoXDTM1MTAwNDIzNTk1
OVowXTELMAkGA1UEBhMCRVMxHDAaBgNVBAoTE1NlY3RpZ28gKEV1cm9wZSkgU0wxMDAuBgNVBAMT
J1NlY3RpZ28gUXVhbGlmaWVkIE5hdHVyYWwgUGVyc29uIENBIEU2NTBZMBMGByqGSM49AgEGCCqG
SM49AwEHA0IAIBCbAj36Fk7EP+pkJmdjD9Q9M/HAW0ZOA91ca5mAYkINyRCCesWtDaLmFyV73z3XQ
Ud2Pg+QgADby67b/8DPq+BGjggFvMIIBazAfBgNVHSMEGDAWgBTH4VKc3GYx9AxP/QqnKDps1e4Q
yzAdBgNVHQ4EFgQUxG4ZAWKtVUvEhNWHyUbLMHmDaGowDgYDVR0PAQH/BAQDAgGGMBIGA1UdEwEB
/wQIMAYBAf8CAQAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMBEGA1UdIAQKMAgwBgYE
VR0gADBQBgNVHR8ESTBHMEWgQ6BHhj9odHRwOi8vY3JsLnNlY3RpZ28uY29tLNlY3RpZ28gRdWFs
aWZpZWROYXR1cmFsUGVyc29uJm9vdEU0NS5jcmwwgYAGCCsGAQUFBwEBBHQwcjBLBggrBgEFBQcw
AoY/aHR0cDovL2NydC5zZWN0aWdvLmNvbS9TZWN0aWdvUXVhbGlmaWVkTmF0dXJhbFBlcnNvbiJv
b3RFNDUuY3J0MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5zZWN0aWdvLmNvbTAKBggqhkjOPQQD
AwNnADBkAjAwIQLvzwkYP+REJb4VSgg+UVQ3ZZ4TTCA35x+syfUQ+RK5OoJ6ipE9KDOmC4gVet0qsC
MAoBkq+4ohbfnPjPDHUZ0tHAz8Di0AopDE/yyHbBkY9QTuOvB3vUSo5JcFcOL++JQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *Sectigo Qualified Natural Person Root E45*

Issuer O: *Sectigo (Europe) SL*

Issuer C: *ES*

Subject CN: *Sectigo Qualified Natural Person CA E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Mon Oct 05 02:00:00 CEST 2020*

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key:

```
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:28:40:8F:7E:85:93:B1:0F:FA:99:09:99:D8:C3:F5:0F:4C:FC:70:16:F1:93:80:F7:57:1A:E6:60:18:90:83:72:44:20:9E:89:6A:C3:68:B9:85:
C9:5E:F7:8B:75:D0:51:DD:8F:83:E4:20:00:36:F2:E9:36:FF:F0:33:EA:F8:11
```

Authority Key Identifier *C7:E1:52:9C:DC:66:31:F4:0C:4F:FD:0A:A7:28:3A:6C:D5:EE:10:CB*

Subject Key Identifier *C4:6E:19:01:62:AD:55:4B:C4:84:D5:87:C9:46:CB:30:79:83:68:6A*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.sectigo.com/SectigoQualifiedNaturalPersonRootE45.crl*

Authority Info Access *http://crt.sectigo.com/SectigoQualifiedNaturalPersonRootE45.crt*

http://ocsp.sectigo.com

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *53:B2:40:05:FD:13:67:1F:54:99:89:C8:C6:69:05:9E:AB:E7:7A:D1:9D:DE:E1:E7:0F:72:C9:FB:B3:C0:D9:F9*

X509SubjectName

Subject CN: *Sectigo Qualified Natural Person CA E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *xG4ZAWKtVUvEhNWHyUbLMHmDaGo=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-05-05T01:00:00Z

43.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

43.5 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Natural Person CA R35”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by “Sectigo Qualified Natural Person CA R35”*

Name *[es]* *Certificados cualificados emitidos por “Sectigo Qualified Natural Person CA R35”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *879009544463711156070572173208599966 82*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGNzCCBB+gAwIBAgIQQiEbp+jhCoHSXam9j9gSCjANBgkqhkiG9w0BAQwFADBlMQswCQYDVQQG
EwJFUzEcMBoGA1UEChMTU2VjdGlnbyAoRXVyb3BlKSBTTDEyMDAGA1UEAxMpU2VjdGlnbyBRdWFs
aWZpZWQgTmF0dXJhbCBQZXJzb24gU m9vdCBSNDUwHhcNMjAxMDA1MDAwMDAwWhcNMzUxMDA0MjM1
OTU5WjBdMQswCQYDVQQGEwJFUzEcMBoGA1UEChMTU2VjdGlnbyAoRXVyb3BlKSBTTDEwMC4GA1UE
AxMnU2VjdGlnbyBRdWFsaWZpZWQgTmF0dXJhbCBQZXJzb24gQ0EgU jM1MIIBojANBgkqhkiG9w0B
AQEFAAOCAY8AMIIBigKCAYEAoAEDUAvfQ7uT+B965DbeLMX8zF04zvlKb44oZFxFq7o1QsLweC2
TJIND/5FLlXEzHjmpg1sJ45zFKh2mRee1ttnhe2zAe1oyMyYwDggmNS/i1GVFL9i4cMVDRMO1IsD
jgWb9M05yjceYDiXiBekm7rT0lERQkEm4eR7ebYRksBkL4 1 19fYgEkmp6cIe2ysa3Io5z/LIHsen
GGEpXGRfpdTfaG1QwHsL4HSDLIjURfjp74mnpO/ukBNwXAnDNow7cVej3UoMPWHvVQf4a5Cb9C
V1o3lmQLdSFf3bcc5LiBoO0zN3p1odcpCKy+tpOT8/t2+L7ZT2CJdK9XBcS/9Kvp1YOO8fLtFqUR
4IV8GaSeKgZLLZRHDEw38xCn7riRra922o+2rfcLojWUpjXKjM2/WQ/LDM92PBYKDZ/oPMwtWhPi
d8a6t5ONiWE3L2SHZE0rMzjC7ju0cAcMprxzIRPS8s43X1/tPeIz14++v+ffOrfdU9//IfGDqjNTU/f
k4mAgMBAAGjggFvMIIBazATBgNVHSMEGDAWgBTk6uFRKjsLSPV49MJICbfCkoQGuTAdBgNVHQ4E
FgQU579kEFIBPKaDCbD8o02jaEBSjQAwDgYDVR0PAQH/BAQDAgGGMBIGA1UdEwEB/wQIMAYBAf8C
AQAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMBEGA1UdIAQKMAgwBgYEVR0gADBQBgNV
HR8ESTBHMEWgQ6BBhj9odHRwOi8vY3JsLnNlY3RpZ28uY29nL1NlY3RpZ29RdWFsaWZpZWROYXR1
cmFsUGVyc29uIm9vdFI0NS5cmwwgYAGCCsGAQUFBwEBBHQwcjBLBggrBgEFBQcwAoY zHR0cDov
L2NydC5zZWN0aWdvLmNvbS9YZWN0aWdvUXVbbGlmaWVkTmF0dXJhbFBlcnNvbIvb3RSNDUuY3J0
MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcCSzZWN0aWdvLmNvbTANBgkqhkiG9w0BAQwFAAOCAgEA
GOEPY/hJfYbO2mfhXDaefwyd8/Di48Y1f+vvnHBHR1OOTawMaP+5mmnKcx0TMB335SkfExhF4NcS+
VdP8VcehksFykWD/7dakyHd7 1J+Vz3Rnf8kCZAUNF7PQg7YaFTVj5ZAqbdC1C wj5MUvRddXUSS
fjB3hKBtcJlnRtpj0/SDKZgruGifvhDo/wGGYPNXbuDu5vDOlrlV7lv0UmBa5obipy2WnCZyeZ3
AOe5tVeTcqqzDZPNQnKqWejS/dcT0WS8IknyQL5WZC6tRSsP00hXuk3sdnmx9fkUrtcc6UOqiAzH
ax4CwdTniojt9B7pjy1HKbgHC/4EsD35OfaU3oidpd14eSYIZvg1SHUUvl5/T1bOjIWhoitZQ
wx4Wx6wwIDimGXXcfTicvfofwIaAofxuNr+pSHfJsLXwnSf5b+vpQLV+amXy9AM6HG2YkZhnzkP
TFIFeXixzqZ9mEUoh1nWFQX9O8GiUxzGYsYEIYKvzTyS Vo8w1zDJaCyjRCwUd7FYJV/pXdBQw+r
jwH/xn/rahSXVbgmbVXam7djwS2W34bi5gO54c96mObUgLD4sfX/cfZQjp2YxAu5tm7Qld1fuTid
gCgFVd9+Mht0ZrJ9KazBEit4x5mw16THHCUJsUmWu6D2xjCKgRqIZkmEHCb5f28XVlpSPYSd4Iw=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer CN: *Sectigo Qualified Natural Person Root R45*

Issuer O: *Sectigo (Europe) SL*

Issuer C: *ES*

Subject CN: *Sectigo Qualified Natural Person CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Mon Oct 05 02:00:00 CEST 2020*

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key:


```
30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:A0:01:03:50:0B:DF:43:BB:6E:4F:E0:7D:EB:90:DB:78:B3:17:F3:31:74:E3:3B:E5:29:BE:38:A1:91:71:16:AE:E8:D5:
0B:0B:C1:E0:B6:4C:92:4D:0F:FE:45:2E:55:C4:CC:78:E6:A6:0D:6C:27:8E:73:14:A8:76:99:17:9E:D6:DB:67:85:ED:B3:01:ED:68:C8:CC:98:C0:38:2A:98:D4:BF:8B:51:95:14:BF:62:E1:C3:15:0D:13:0E:D6:5B:03:8E:05:9B:
F4:CD:39:CA:37:1E:60:38:97:7C:17:A4:9B:BA:D3:38:44:50:90:49:B8:79:1E:DE:6D:84:64:B0:19:0B:E3:5D:7D:7D:88:04:92:7A:7A:72:22:5E:DB:2B:1A:DD:FA:39:CF:F2:C8:1E:C7:A7:18:61:29:5C:64:65:A5:D4:DF:68:6D
:50:C0:7B:0B:E0:7E:43:2E:58:D4:45:F8:E9:EF:89:EB:BA:93:BF:BA:40:4D:C1:70:27:0C:DA:30:4D:C5:5E:8F:72:14:A0:C3:D6:1E:F5:50:23:86:B9:09:BF:42:57:5A:37:22:64:0B:75:21:5F:DD:B7:1C:E4:B8:81:A0:ED:33:37:
7A:75:A1:D7:29:08:AC:BE:B6:93:93:F3:FB:76:F8:BE:D9:4F:60:89:74:AF:57:05:C4:BF:F4:AB:E9:D5:83:8E:F1:F2:ED:16:A5:11:E0:85:7C:19:A4:9E:2A:06:4B:2D:94:47:0C:4C:37:F3:10:A7:EF:38:91:AD:AF:76:DA:8F:B6:
AD:F7:8B:A2:35:94:A6:35:CA:8C:CD:BF:59:0F:CB:0C:CF:76:3C:16:0A:0D:9F:E8:3C:CC:2D:5A:13:E2:77:C6:BA:B7:93:8D:89:61:37:B7:64:87:64:43:AB:33:38:C2:EE:3B:B4:B0:07:0C:A6:BC:73:95:13:D2:F1:AE:37:5F:5
F:ED:3D:E7:F3:D7:8F:AF:F9:F3:AB:7D:D5:3D:FF:F2:1F:18:3A:A3:35:35:1F:93:88:A7:02:03:01:00:01
```


Authority Key Identifier *E4:EA:E1:45:46:3B:0B:48:F5:78:F4:C2:49:09:B2:42:92:84:06:B9*

Subject Key Identifier *E7:BF:64:10:52:01:3C:A6:83:09:B0:FC:A3:4D:A3:68:40:52:8D:00*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.sectigo.com/SectigoQualifiedNaturalPersonRootR45.crl*

Authority Info Access *http://crt.sectigo.com/SectigoQualifiedNaturalPersonRootR45.crt*

http://ocsp.sectigo.com

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AC:86:68:30:D7:B8:D7:12:73:C7:CD:E0:57:A8:D5:3E:93:4C:4E:6F:16:94:7D:13:8A:12:3C:BE:C8:C6:3B:DE*

X509SubjectName

Subject CN: *Sectigo Qualified Natural Person CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *579kEFIBPKaDCbD8o02jaEBSjQA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-05-05T01:00:00Z

43.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

43.6 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Legal Person CA E35”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by “Sectigo Qualified Legal Person CA E35”*

Name *[es]* *Certificados cualificados emitidos por “Sectigo Qualified Legal Person CA E35”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *254327536966584965713359262860379861960*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDRDCCAsmgAwIBAgIRAL9Vs7CLooq60nHi7ySSs8gwCgYIKoZIzj0EAwMwXTELMAkGA1UEBhMC
RVMxHDAaBgNVBAoTE1NlY3RpZ28gKEV1cm9wZSkgU0wxMDAuBgNVBAMTJ1NlY3RpZ28gUXVhbGlm
aWVkIExlZ2FsIFBlcnNvbiBSb290IEU0NTAeFw0yMDEwMDUwMDAwMDBaFw0zNTEwMDQyMzU5NTla
MFsxCzAJBgNVBAYTAkVTMRwwGgYDVQQKExNTZWNtaWdvICJpZXMxMS4wLAYDVQQDEyVT
ZWN0aWdvIFF1YWxpZmllZCBMZWdhbCBQZXJzb24gQ0EgRTM1MFkwEwYHKoZIzj0CAQYIKoZIzj0D
AQcDQgAELs1kgTX/HVayQc4Ax/CbLanGms6R0HRTG4vUuHGbM/GpVmvxljix6Zen5lhQR9tm4B4y
ITXEG3YsXS6EVjz+3aOCAWowggFmMB8GA1UdIwQYMBaAFA7Jn2M+Gd4m+mM/jDYQICzREoqMB0G
A1UdDgQWBBRQP2M1YSSWGd7xzXeoqAt1crsVYzAOBgNVHQ8BAf8EBAMCAYYwEgYDVR0TAQH/BAgw
BgEB/wIBADAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwEQYDVR0gBAowCDAGBgRVHSAA
ME4GA1UdHwRHMEUwQ6BBoD+GPWh0dHA6Ly9jcmwuc2VjdGlnby5jb20vU2VjdGlnbl1F1YWxpZmll
ZExlZ2FsUGVyc29uUm9vdEU0NS5jcmwwfgYIKwYBBQUHAQEEcjBwMEkGCCsGAQUFBzAChj1odHRw
Oi8vY3J0LnNlY3RpZ28uY29tL1NlY3RpZ28gRWFsaWZpZWRMZWdhbFBlcnNvbUlvb3RFNDUuY3J0
MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcCSzZWN0aWdvLmNvbTAKBggqhkjOPQQDAwNpADBmAjEA
obHhe8KA3wKC7p4eqpHDcRcfnQ+Cmvh37TkNXa1JzgfEs3a7lYS1doszkFvlKvoIAjEAq3k8mN/y
W+Z5iM6AKvO14ge8GqLFFuycmaMjwZPR2xieCyWOtpNg9GE2mAkY/lb
-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *Sectigo Qualified Legal Person Root E45*

Issuer O: *Sectigo (Europe) SL*

Issuer C: *ES*

Subject CN: *Sectigo Qualified Legal Person CA E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Mon Oct 05 02:00:00 CEST 2020*

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key:

```
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:2E:CD:64:81:35:FF:1D:56:B2:41:CE:00:C7:F0:9B:2D:A9:C6:9A:CE:91:D0:74:53:1B:8B:D4:B8:71:9B:33:F1:A9:56:6B:F1:96:38:B1:E
9:97:A7:E6:58:50:47:DB:66:E0:1E:32:21:35:C4:1B:76:2C:5D:2E:84:56:3C:FE:DD
```

Authority Key Identifier *0E:C9:9E:2D:8C:F8:67:78:9B:E9:8C:FE:30:D8:40:80:B3:44:4A:2A*

Subject Key Identifier *74:3F:73:35:63:94:96:1B:8E:F1:CD:77:A8:A8:0B:75:72:BB:15:63*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.sectigo.com/SectigoQualifiedLegalPersonRootE45.crl*

Authority Info Access

http://crt.sectigo.com/SectigoQualifiedLegalPersonRootE45.crt

http://ocsp.sectigo.com

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D1:1D:91:67:B7:6C:CF:32:AF:9F:FE:0D:5B:F6:6A:82:BB:56:85:40:AE:39:F5:96:54:41:FB:BD:55:E1:D9:D8*

X509SubjectName

Subject CN: *Sectigo Qualified Legal Person CA E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *dD9zNWOUlhuO8c13qKgLdXK7FWM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-05-05T01:00:00Z

43.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

43.7 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Legal Person CA R35”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by “Sectigo Qualified Legal Person CA R35”*

Name *[es]* *Certificados cualificados emitidos por “Sectigo Qualified Legal Person CA R35”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *281853815834614069450094829868643163637*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGLzCCBBcgAwIBAgIRANQLEgTJ5FEydXaLZE96mfUwDQYJKoZIhvcNAQEMBQAwXTELMAkGA1UE
BhMCRVMxHDAaBgNVBAoTE1NlY3RpZ28gKEVlcm9uZSkgU0wxMDAuBgNVBAMTJ1NlY3RpZ28gUXVh
bGlmaWVkIExlZFsIFBlcmNvbiBlSb290IF0NTAeFw0yMDEwMDUwMDAwMDBaFw0zNTEwMDQyMzU5
NTlaMFsxCzAJBgNVBAYTAkVTMRwwGgYDVQQKExNTZWN0aWdvIChFdXJvcGUpIFNMMMS4wLAYDVQQD
EyVTZWN0aWdvIFF1YWxpZmllZCBMZWdhbCBQZXJzb24gQ0EgUjM1MIIBojANBgkqhkiG9w0BAQEF
AAOCAY8AMIIBigKCAYEAyJxmTmn+aZogwPjdlbawkeYYib/2iGL1yrIiZzI88PmGthIYZmvQunlmS
/+FoSQcV/QcPnl+Vj14Hdrc9+xxSZRtHAcq+5oJf1tYWP6doE98sXWfV6jtuzSeLTdWqvIWpz
ueoFiL2dlNwoLY0SU8ytXdsimXUO4kiYytlF2KNqTyl8EwvIGCbWPDwAPXOHIu/Xx3sTZACMjG0n
wZ6MKMbm2RUjl0GdLNBwg9IJMvFvb0SDDOVd3xe6HQp+C528HonZyNbYrkJ4sAFS1VPv7VvCg7BP
hqNZjdg0WM5EyyRn1r+1O5m8sxSnHYjR5qaMrRQGbCXian5Eqydkxdgksh2el6OcOGMcwvxVEW1
IvkAkb+ZH1cfq16bKcsdrMRp+talS4X9xJpCS1g2Gvuq5zRlbKqZuSigT5bAfE0+fp3N7GYtL0Ip
R9fuuW21xcUjCapCnom3/yqCoTmdWspP/iuqxHpEXr1+EVHq6Bvw1.hhp3DXBURBVQH0z/rB9Ub3t
AgMBAAGjggFqMIIBZjAfBgNVHSMEGDAWgBQHS3Qv13BKeeLPyKqmaQWACIMHajAdBgNVHQ4EFgQU
rO4i+LmLSe5yExqRb6TiTiTU7BQwDgYDVR0PAQH/BAQDAgGGMBIGA1UdEwEB/wQIMAYBAf8CAQAw
HQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMBEGA1UdIAQKMAgwBgYEVR0gADBOBgNVHR8E
RzBFMEOgQaA/hj1odHRwOi8vY3JsLnNlY3RpZ28uY29tL1NlY3RpZ29RdWFsaWZpZWRMZWdhbFBl
cnNvbUvb3RSNDUuY3JsMH4GCCsGAQUFBwEBBHIwcDBJBggrBgEFBQcwAoY9aHR0cDovL2NydC5z
ZWN0aWdvLmNvbS9TZWN0aWdvUXVhbGlmaWVkTGVnYWxQZCUzb25Sb290IjQ1LmNydDAjBggrBgEF
BQcwAYYXaHR0cDovL29jc3Auc2VjdGlnby5jb20wDQYJKoZIhvcNAQEMBQADggIBAFkLbSrJ5nd
72pO/pHBOsm72JqwJIYJxGUNJDF8VI2mWElwJOSsrU6eDvTsLdU3V4q/eCEGxIk404jOZVPPJoR
YXpXfuYbLu0uuwhGX3mHS5/dw16jWeCl2rj9uihpQtZNtzhtky1xmKMAg46zWwqBApjB5oayLt2g
y0+XJbFYbqkyrDspZMPjMJmJfgdGg6xt7mmVP9aEi/4bXw2zMyAORtyQY7tuzSm8Gc+2Yjasq5f89
o8kpDKzKPmzYTMUFRASVcFdcuVj6Mt0+s6ZcGslxSEQpZ6xQPQU+3GNG+4o1UGLNYD6Oquy5sII9
ewfsESxzDFHYhle798sa9ub9b2bnpL3Ibjtm93jnKcYHCILANcBgSBx3zhhzs87eiNMB9Rm75zqr
eSy/OYxJaca3zcdZIsBT8KhmsG3dATW59XK3gDreeUv8P/ZvNH6sDIcwg0VjvL9vSWavYJgiDcos
OP0EFR2d1jwcZRz91vYX9wwzyajUL34MSqOlGYROG++ON+JrHHpCv2VSOZRJIBNBRYyUxY1SRoE
Eo16juhaWWbzHJluRJSqPD8DdPFm1xTCTGAzeeTbFhh5o07HHvXYJZbVhmDZ/jWR2v8hr6ku92Km
tYal7wINBIu+bxmQ7Pq7IlIDCLCopqytbjGlRzOrL6dpCFCMjM9cy8l4hZuMHEAIrE

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer CN: *Sectigo Qualified Legal Person Root R45*

Issuer O: *Sectigo (Europe) SL*

Issuer C: *ES*

Subject CN: *Sectigo Qualified Legal Person CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Mon Oct 05 02:00:00 CEST 2020*

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:C8:9C:66:4E:69:FE:69:9A:20:C0:F8:DD:85:B6:B0:91:C6:18:89:BF:F6:88:62:F5:CA:B2:22:67:30:7C:3E:61:9F:84:86
:19:9E:F4:2E:9C:89:92:FF:E1:68:E5:07:95:FC:E7:0F:9E:5F:95:8F:5E:07:89:DA:DC:F7:EC:71:E5:94:6D:1C:07:2A:FB:9A:3F:17:5B:55:7D:63:FA:76:81:3D:F3:15:D6:7D:5E:A5:8E:D6:B3:E5:E2:D3:75:6A:B2:21:6A:73:B9:
EA:05:88:BD:9D:7C:DC:28:2D:8D:12:53:CC:AD:5D:DB:22:99:75:0E:E2:48:98:CA:D2:05:D8:A3:6A:4F:29:7C:13:0B:E5:18:26:D6:3C:3C:00:3D:73:87:22:EF:D7:C7:7B:13:64:00:8C:8C:6D:27:C1:9E:8C:28:C6:E6:D9:15:23
:23:41:9D:2C:D0:70:83:D2:09:32:F1:6F:87:44:83:0C:E5:5D:DF:17:BA:1D:0A:7E:0B:9D:BC:1E:89:D9:C8:D8:58:AE:49:78:B0:01:52:D5:53:EF:ED:5B:C2:83:B0:4F:86:A3:59:8D:D8:34:58:CE:44:CB:24:67:D6:BF:B5:3B:99
:BC:B3:14:A7:1D:88:D1:E6:A6:8C:AD:14:06:84:25:D7:89:A9:F9:12:AC:9D:93:17:60:92:C8:76:7A:5E:8E:70:E1:8C:73:0B:F1:54:45:B5:96:F9:00:91:BF:99:1F:57:1F:A8:8E:9B:29:CB:1D:AC:C4:69:FA:D6:88:4B:85:FD:C6:
5A:42:4B:58:36:1A:FB:A0:E7:34:65:87:CA:99:B9:28:A0:4E:C6:C0:7C:4D:3E:7E:9D:CD:EC:66:2D:2F:FD:29:47:D7:EE:B9:6D:B5:C5:C5:23:09:AA:42:9E:89:B7:FF:2A:82:A1:39:9D:5A:CA:4F:FE:2B:AA:C4:7A:44:5E:B2:
3E:11:51:EA:E8:1B:F0:2E:18:69:DC:35:C1:51:10:55:40:7D:33:FE:B0:7D:51:BD:ED:02:03:01:00:01

Authority Key Identifier *07:4B:74:2F:D7:70:4A:79:E2:CF:C8:AA:A6:69:05:80:08:83:07:6A*

Subject Key Identifier *AC:EE:22:F8:B9:8B:F1:EE:72:13:1A:91:6F:A4:E2:4D:F2:14:EC:14*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.sectigo.com/SectigoQualifiedLegalPersonRootR45.crl*

Authority Info Access

http://crt.sectigo.com/SectigoQualifiedLegalPersonRootR45.crt

http://ocsp.sectigo.com

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *33:95:96:69:16:F8:D3:9D:CE:B5:F7:5C:FF:8B:8E:F4:ED:CB:36:2B:1C:0C:27:92:4D:A4:2D:07:DD:18:F1:59*

X509SubjectName

Subject CN: *Sectigo Qualified Legal Person CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *rO4i+LmL8e5yExqRb6TiTfIU7BQ=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-05-05T01:00:00Z

43.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

43.8 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Website Authentication CA Natural E35”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by “Sectigo Qualified Website Authentication CA Natural E35”*

Name *[es]* *Certificados cualificados emitidos por “Sectigo Qualified Website Authentication CA Natural E35”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *138773655142807905223248947672508247733*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDdDCCAvugAwIBAgIQaGbVc3fvdIfagmignj+utTAKBggqhkjOPQQDAzCBiDELMAkGA1UEBhMC
VVMxEzARBgNVBAgTCk5ldyBKZXlzZXkxFDASBgNVBAcTC0plcnNleSBDaXR5MR4wHAYDVQQKExVU
aGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNVBAMTJVVTRVJUcnVzdCBFQ0MgQ2VydGlmaWNhdGlv
biBkdXRob3JpdHkwHhcNMjAxMTE3MDAwMDAwWhcNMzUxMTE2MjM1OTU5WjBtMQswCQYDVQQGEwJF
UzEcMBoGA1UEChMTL2YqK2lnbyAoRXVyb3BlKSBTTTDFAMD4GA1UEAxM3L2YjdGlnbyBRdWFsaWZp
ZWQgV2Vic2l0ZSBBdXRoZW50aWNhdGlvbiBDQSBOYXR1cmFsIEUzNTBZMBMGByqGSM49AgEGCCqG
SM49AwEHA0IABCQzEZK6e64f9fcv4Vm51++8RKtzZt9TApgcW+zVNLBM5N3YBvmjb41s708BiVNb
+5RVj0SOOFAAZ1+HSpcW6NGjggFfMIIBWzAfBgNVHSMEGDAWgBQ64QmG1M8ZwpZ2dEl23OA1xmNj
mjAdBgNVHQ4EFgQUVy25hdRFr+aT12b1N+s/HmAHHaAwDgYDVR0PAQH/BAQDAgGGMBIGA1UdEwEB
/wQIMAYBAf8CAQAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEGA1UdIAQKMAgwBgYE
VR0gADBQBgNVHR8ESTBHMEWgQ6BBhj9odHRwOi8vY3JsLnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0
RUNDQ2VydGlmaWNhdGlvbkF1dGhvcml0eS5jcmwwcQYIKwYBBQUHAQEEZTBjMDoGCCsGAQUFBzAC
hi5odHRwOi8vY3J0LnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0RUNDQUFBQ0EuY3J0MCUGCCsGAQUF
BzABhhlodHRwOi8vb2NzcC51c2VydHI1c3QuY29tMAoGCCqGSM49BAMDA2cAMGQCMEQ4Gid0C+xyj
CQVSCDuZ3cgsYEEpyBZsNjmdLtpvNhSISieNy1dLkaaE1UoVPIEjbgIwbuRK+OThKs5/A13n7j9/
Ra5KmQn+92zVZ3oxcX0ytAjOMiZxEAFMvfMaRVGum/G8

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *USERTrust ECC Certification Authority*

Issuer O: *The USERTRUST Network*

Issuer L: *Jersey City*

Issuer ST: *New Jersey*

Issuer C: *US*

Subject CN: *Sectigo Qualified Website Authentication CA Natural E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Tue Nov 17 01:00:00 CET 2020*

Valid to: *Sat Nov 17 00:59:59 CET 2035*

Public Key:

```
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:24:33:11:92:BA:7B:AE:1F:F5:F7:2F:E1:59:B9:D7:EF:BC:44:AB:73:66:DF:53:02:98:1C:5B:EC:D5:34:B0:4C:E4:DD:D8:06:F9:A3:6F:
8D:6C:EF:4F:01:89:53:5B:FB:94:55:8F:44:8E:38:50:00:67:5F:87:4A:97:16:E8:D1
```

Authority Key Identifier *3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A*

Subject Key Identifier *57:2D:B9:6D:D4:5F:FB:E6:93:23:66:F5:37:EB:3F:1E:60:07:1D:A0*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_serverAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl*

Authority Info Access *http://crt.usertrust.com/USERTrustECCAAACA.crt*

http://ocsp.usertrust.com

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A9:84:1D:2E:47:CB:E6:D7:1D:8F:AF:DF:38:38:7F:93:F4:3D:76:D7:92:50:4E:FB:17:A2:10:20:C5:8C:0B:89*

X509SubjectName

Subject CN: *Sectigo Qualified Website Authentication CA Natural E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *Vy25bdRf++aTI2b1N+s/HmAHHaA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-05-05T01:00:00Z

43.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

43.9 - Service (granted): Qualified Certificates issued by "Sectigo Qualified Website Authentication CA Natural R35"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by "Sectigo Qualified Website Authentication CA Natural R35"*

Name *[es]* *Certificados cualificados emitidos por "Sectigo Qualified Website Authentication CA Natural R35"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *178407546750340678743431264725430973998*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGYjCCBEqgAwIBAgIRAIY4Cy0+ZbmAEDBlHg50Ni4wDQYJKoZIhvcNAQEMBQAwgYgxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIEwpOZXcgSmVyc2V5MRQwEgYDVQQHEwtKZXJzZXlsQ2l0eTEeMBwGA1UE
ChMVVGhlIFVTRVJUUlVTVCBOZXR3b3JrMS4wLAYDVQQDEyVVU0VSVHJ1c3QgUlNBIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5MB4XDTIwMTExNzAwMDAwMFoXDTM1MTExNjIzNTk1OVowbTELMAkGA1UE
BhMCRVMxHDAaBgNVBAoTE1NlY3RpZ28gKEV1cm9wZSkgU0wxQDA+BgNVBAMTN1NlY3RpZ28gUXVh
bGlmaWVkIFdlYnNpdGUgQXV0aGVudGljYXRpb24gQ0EgTmF0dXJhbCBSMzUwggGiMA0GCSqGSIb3
DQEBAQUAA4IBjwAwggGKAoIBgQCS4LLVDvbssJS2PweSixvfCBGazQ7TznTNK92y/ugYCMD5rfZV
eBhaAg8p3arP5nGGN2iJUVdNoKpWcqSWKu4qV8DM8t6T1F7/MbbZj6uG+pNqtwv5WGiOnozxRZ
faR0T+9DBs6S8SrlIbPWprnBcypp2eHK4qWXMv+qqDNEJm+mlSEkMdhzcI/GvvGb8p6sBpGAD
S61/fvQUzBM3lVTIX4ESj4DZpzX+1p/yPmefCn639KidHzIL G0lGW1KYkCXifbHZYQR3uBTF3sd
6sfyv7TiwdIj8m436eBpjGYMjlCQ2n25YctZg975wD1t/h3ZlWpXanchPxIRqE6npza2mXFuaOA
qqZHQsJ1wDN4wV5Ml/5SWS009bU1y91Z6sF9MX038eLxoqm2UGzWzs0A5nCq4ZLGd0ngtYOD13M
EgPegtxKBt3g8HEqsUHPHR2ARBw1rvAQYeLv5VQKckk58uc4aLzGXd5qm2dkqYhXgvQeldTbcn
XeloebcCAwEAAaOCAV8wggFbMB8GA1UdIwQYMBaAFFN5v1qqK0rPVIDh2JvAnfKyA2bLMB0GA1Ud
DgQWBBT11tBBwktAxHKBpT4tGVjpWyUpODAOBgNVHQ8BAf8EBAMCAYYwEgYDVR0TAQH/BAgwBgEB
/wIBADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEQYDVR0gBAowCDAGBgRVHSAAMFAG
A1UdHwRJMEcwRaBDoEGGPzJodHA6Ly9jcmwudXNlcnRydXNlcnRvb3VlOVSVHJ1c3RSL0fDZXJ0
aWZpY2F0aW9uQXV0aG9yaXR5LmNybDBxBggrBgEFBQcBAQRlMGMwOgYIKwYBBQUHMAKGLmh0dHA6
Ly9jcnQudXNlcnRydXN0LmNvbS9VU0VSVHJ1c3RSU0FBQUFDQS5jcnQwJQYIKwYBBQUHMAGGGWh0
dHA6Ly9vY3NwLnVzZXJlcnVzdC5jb20wDQYJKoZIhvcNAQEMBQADggIBADPL THB1IB0tRFzMLGQG
vNWYeFUjYkHv+X6HuGikfj2RZCAdbt7dDs9BChxkKExJnIdSdbynz7WHngZxWS6M7fvRgUVjgIGN1
LaQeR/yrcASXaQfVnB93oOB0QMpghrQ7FS6ZruY8QrMp7hmb6HHK7b/AD3kgcco T8Noen8RUvydR
ManKJlvPkGl4TnnCZ7UvozU/qux/lZ7NvQ6G6vHlvOSssJZhZ/MnFnuykuSGYgp4CWvd97f0uTX6e
1FNROGRLPtpx34O+BGc2lvR2vqBO6xx2nBt9qSJLk5klUJ6c+YbO1bAxIK57ciUrSOXArsy/S4A
ET0B7o0rhAL+e8E9qdiZbMGdmEPfjc3Vjn0RUi4QfpOZo4TKEDnb8ToXoOXFk6zm1TWuiIUSwld6g
7oS2srPHOKZOvi3d091g117yup4PqsCFvuPxODAcZNxsdBB2kOoc3r7qTsoFcxzGPi1XzDVbw
WlrUiNTiXD1TWKzZGfcswT4dStLM3Pw59gp+EpYrV3oB0H1GqM/MFOyxHFityo1ehvaNB4lHYGe
8D0mgfzNTdky2lQ4EENvbhYBpsWzze79R7QvJwaZ+W1SLLxlkEnsUp0xizT2XocVIMDHJ8A1fjd
Gp9dfaR8QKFR+qbhrSW5SasYkfxjjgVlX96c0ekGNRUewsKFKEzk16QT

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer CN: *USERTrust RSA Certification Authority*

Issuer O: *The USERTRUST Network*

Issuer L: *Jersey City*

Issuer ST: *New Jersey*

Issuer C: *US*

Subject CN: *Sectigo Qualified Website Authentication CA Natural R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Tue Nov 17 01:00:00 CET 2020*

Valid to: *Sat Nov 17 00:59:59 CET 2035*

Public Key:


```
30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:92:E0:B2:D5:0E:F6:EC:B0:94:B6:3F:07:92:8B:1B:DF:08:11:9A:CD:0E:D3:CE:74:CD:2B:DD:B2:FE:E8:18:08:C0:F
9:AD:F6:55:78:16:DA:02:0F:29:DD:AA:CF:E6:71:86:37:68:88:25:57:4D:A0:AA:56:72:A4:96:2A:EE:2A:57:C0:CC:F2:DE:93:FE:D1:53:FF:D3:1B:6D:98:FA:B8:6F:A9:36:AB:70:BF:95:86:88:E9:E8:CF:14:59:7D:A4:74:4F:
EF:4E:06:CE:92:F2:24:AB:96:56:CF:5A:9A:E7:05:CC:A9:A7:67:87:2B:8A:96:95:73:2F:FA:AA:83:34:42:66:FA:69:52:12:43:22:87:37:08:FE:21:AF:BC:68:7C:A7:AB:01:A4:60:03:4B:AD:7F:7E:F4:14:CC:13:37:21:54:E5:5F
:81:12:8F:80:D9:A7:35:FE:D6:9F:ED:C8:F9:9E:7C:29:FA:DF:D2:A2:74:7C:C8:2C:6D:25:19:6D:4A:62:40:97:89:F6:C7:65:84:11:DE:E0:53:17:7B:1D:EA:C7:F2:BF:B4:DF:C2:27:48:8F:C9:B8:DF:A7:81:A6:31:98:32:39:42:
43:69:F6:E5:87:1F:DA:0F:7B:E7:00:F5:B7:F8:77:66:55:A9:5D:A9:DC:84:FC:48:46:A1:3A:9E:9C:DA:DA:65:C5:B9:A3:80:AA:A7:F6:1D:0B:09:D7:00:CD:E3:05:79:31:4E:52:59:2D:34:F5:B5:35:CB:DD:6D:67:AC:85:F4:C
5:F4:DF:C7:8B:C6:8A:A6:D9:41:B3:5B:3C:74:03:99:C2:AB:86:4B:19:DD:27:82:D6:0E:0F:5D:CC:12:03:DE:8A:0B:71:28:18:F7:83:C1:C4:AA:C5:07:3C:87:CE:D8:04:41:C3:5A:EF:01:05:5E:2E:FE:55:40:A7:24:93:9F:2E:7
0:06:8B:CC:63:9D:E6:A9:B6:76:4A:95:85:78:2F:41:C9:5D:4E:17:27:5D:E9:68:79:B7:02:03:01:00:01
```


Authority Key Identifier *53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB*

Subject Key Identifier *E5:D6:D0:41:C2:47:C0:C4:72:81:A5:3E:2D:19:58:E9:5B:25:29:38*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_serverAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl*

Authority Info Access	*http://crt.usertrust.com/USERTrustRSAAAACA.crt* *http://ocsp.usertrust.com*
Key Usage:	*digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*33:9E:6B:92:BE:54:59:F2:6A:8D:C3:C5:F3:72:09:33:C8:38:E2:36:60:1B:05:00:48:C0:47:A1:23:E6:F8:E7*

X509SubjectName

Subject CN:	*Sectigo Qualified Website Authentication CA Natural R35*
Subject O:	*Sectigo (Europe) SL*
Subject C:	*ES*

X509SKI

X509 SK I	*5dbQQcJHwMRygaU+LRlY6VslKTg=*

Service Status		*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Service status description	*[en]*	*undefined.*
	[es]	*undefined.*
Status Starting Time		*2021-05-05T01:00:00Z*

43.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

44 - TSP: Docuten Tech SL

.

TSP Name

Name	[en]	Docuten Tech SL
Name	[es]	Docuten Tech SL

TSP Trade Name

Name	[en]	Docuten
Name	[es]	DOCUTEN TECH SL
Name	[en]	VATES-B85630978

PostalAddress

Street Address	[en]	C/ GAMBRINUS 7,1º D
Locality	[en]	A CORUÑA
Postal Code	[en]	15008
Country Name	[en]	ES

ElectronicAddress

URI	[en]	mailto:administracion@docuten.com
URI	[en]	https://docuten.com/en
URI	[es]	https://docuten.com/es

TSP Information URI

URI	[en]	https://docuten.com/en/pcsc/

44.1 - Service (granted): Certificados cualificados emitidos por “DOCUTEN TECH CA1”

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name *[es]* *Certificados cualificados emitidos por “DOCUTEN TECH CA1”*

Name *[en]* *Qualified Certificates issued by “DOCUTEN TECH CA1”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3425867390684835747*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIajCCBlKgAwIBAgIIL4sgPaVdL6MwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRswGQYDVQQDDBJVQU5BVEFDQSBST09UIDIwMTYxGDAWBgNVBGEMD1ZBVETLUE2NjcyMTQ5OTAe
Fw0yMDA5MTgwODUyMjFaFw0zMzA5MTgwODUyMjFaMIGKMQstCQYDVQQGEwJFUzESMBAGA1UEBwwJ
QSBDT1JVw5FBMRgwFgYDVQQKDA9Eb2N1dGVuIFRlY2ggU0wxGDAWBgNVBAsMD1RTUC1QU0MtRE9D
VVRFTjEZMBcGA1UEAwwQRE9DVVRFTiBURUNlIENBMTEYMBYGA1UEYQwPVkFURVMtQjg1NjMwOTc4
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEArKkEXyZTsfo6yaYnsdQouP3dVPTFJsQ
QSo1rutBhKA7IEAvK3FB1BZW8ID3vd4IRBjTbrupiQ3bDp3tmnNTD6pSgQvG50G2umctSPaQ1ZPv0V
FtbYl/tsq/K+BP6NbaxV39+fe9x8+pQW8Jc9NxiKdnXxoA3M6l7MeXiNkiJk/gPVqheb2Y8FGMS
8FugJUKkQMqiKzWpdwO1aw2HGNIDEGdek7mntKOLbUZxgAOG6nc/7DyJ9p2F/L6kWekS7TypkZ5z
0edsiSeh5tXky9P0Ss7pw08DH0E1IOA9sz8H3rbiQH7RBf0MxyNqVVKAhR/NZXgXM/CTcwYZWuqj
JODlo76RsyVzywBleNT21Ebv+WCbKMRcwY+NpqRxAUYPDyUvHkTVCuesf72mbFaG5ZN+j0MtUi
QSkRDg6T6g7j3UMAIDO2EC8xWFctvSNEb4BUnu57nbYFBboKjmwES+72wUBsPLgBEaHCpD+rxGZ
tTomO6Pr5c7dDXhnZBb4YTjt05x9gWSoY9LfaG4DAjlopeTtUNx3JO57QmokXA9gMO9RYwqIajXb
A+DtPuCycx88atyt4tT8rR2+rcPg4FiZjoegSU/jMNcplPPf7FQDw7QqdXgpuO9FcAhccuycPnig
QdAjWwiP5TIH47fBNoBnjw2/Nq8/8UNgaRcakGjNx+sCAwEAAaOCAgEwggKdMH4GCCsGAQUFBwEB
BHIwcDA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpl.29j
c3AvMDYGCCsGAQUFBzABhipodHRwOi8vb2NzcDludWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2Nz
cC8wHQYDVR0OBBYEFHDjJf5NqXI/UYDWInpHYpJmLr9YMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYD
VR0jBBgwFoAUVSzvvKFeue6gLdhXEfv8lveRmnwwHAYDVR0SBBUwE4ERaW5mb0B1YW5hdGFjYS5j
b2Mwgc0GA1UdLASBSTCBsjCBs3wYEVR0gADCBr1JAwBggrBgEFBQcCARYkaHR0cHM6Ly93d3cuZG9j
dXRlbi5jb20vZXMvcGNzYy9jcHMvMIGhBggrBgEFBQcCAjCBlAyBkVN1Ym9yZGluYXRlIENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IENlcnRpZmljYWNpb24gU3Vib3JkaW5hZGEgZGUgLyBEb2N1dGVuHRIY2ggL.SB3
b3JpZGFkIGRlIENlcnRpZmljYWNpb24gU3Vib3JkaW5hZGEgZGUgLyBEb2N1dGVuHRIY2ggL.SB3
dXcuZG9tdXRlbi5jb20wgYsGA1UdHw5Bgz CBgDA+oDygOoY4aHR0cDovL2NvbDEudWFuYXRhY2Eu
Y29tL3B1YmxpYy9wa2kvY3JsL2FybF91YW5hdGFjYS5jcmwwPqA8oDqGOGh0dHA6Ly9jcmwyLnVb
bmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NvbC9hcmxfdWFuYXRhY2EuY3JsMA4GA1UdDwEB/wQEAwIB
BjAbBgNVHREEFDASgRBpbmZvQGRvY3VOZW4uY29tMA0GCSqGSIb3DQEBCwUAA4ICAQBgd75pSyoG
HA1bFuGiUlgYRYINsrwufspcfo8Q94Tce2IPc5naGi5bptBj22d5pZaDFH34tPTNkOfcgCSCn
XBTg2QZWjiuz29gjxF746bp3ZGu82FlXVrSl+wFrFlYZJeehjCCiq+fVvDwqbAPPYO0CqYzTUeis
ZHMQAFSf1e1md2SB5E50Z4P516TOJpmNlWIUjtXiapqrgIksadQoHQNSA/adzB8ZhMoFnYerrMYg
BTa/Rh+YsE+z6VwggelaW8VpraLrqUp/AdmWW58BwuBBnrpwd04ZR9eQNiJgcqcEOzrChiyhSsbd
WYh6IWJL Y9f6qRIJ2v7ySXcvCArAdtU56RTNJlh/QZ99U5/sD+tjbsbAgIbX7JivNXzrRgPYGtJ
Y5ZFpr6qJOGN4IdXscIY8olHuYal1GVrDT0HOXQqWUnNejAwQvipcuRvCTcWI5WdJXXCkwybCwHw
Vyp3z2zt+QRua4D/+iqwVMXjvtS3G86Np+IS606OE/OpBAVqMVbg1Ugvd4/MU/OUpCbRtfbQdkguj
xuVW6AZVDn78e91e7Xjo95tr5HDj+zRIozdvvoJBNyO00TYowJQLacxv1yYTI6gCZSx2tWwdqxtm
YilZmWd2A+/78dlla37TZdLBg2Y6lTIidK+aWFH5MEulc7exdsmRUKxlwVCHUgELA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA ROOT 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B85630978*

Subject CN: *DOCUTEN TECH CA1*

Subject OU: *TSP-PSC-DOCUTEN*

Subject O: *Docuten Tech SL*

Subject L: *A CORUÑA*

Subject C: *ES*

Valid from: *Fri Sep 18 10:52:21 CEST 2020*

Valid to: *Sun Sep 18 10:52:21 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AD:19:04:5F:26:53:B1:FA:3A:C9:A6:27:B1:D4:28:B8:FD:DD:54:F4:C5:26:3B:10:41:2A:35:AE:E0:61:28:0E:C8:10:0B:CA:DC:50:75:F1:95:BC:D4:32:6F:E1:F4:41:8D:33:AB:BA:98:90:DD:B0:E9:DE:69:8D:EC:3E:A9:4A:04:2F:1B:9D:06:DA:E9:9C:B5:23:DA:43:56:7F:3E:FD:15:16:DB:58:97:FB:6C:AB:F2:BE:04:FE:8D:6D:AC:55:DF:DF:9F:7B:DC:7C:FA:94:16:F0:97:3D:37:18:8A:76:75:F1:A0:0D:CC:EA:5E:CC:79:7B:4D:92:22:23:93:F8:0F:56:A8:5E:6F:66:3C:14:63:12:F0:5B:A0:8D:42:A4:40:CA:A2:2B:35:A9:77:03:B5:6B:0D:87:18:D2:03:10:67:5E:93:B9:A7:B4:A3:8B:6D:46:71:80:03:86:EA:77:3F:EC:38:C8:F6:9D:85:FC:BE:A4:59:E9:12:ED:3C:A9:91:9E:73:D1:E7:6C:89:27:A1:E6:D5:E4:CB:D3:F4:4A:CE:E9:C3:4F:03:1F:41:35:94:E0:3D:B3:3F:07:DE:B6:E2:40:7E:D1:05:F2:4C:C7:23:6A:55:52:80:85:1F:CD:65:78:17:33:F0:93:7B:06:19:5A:EA:A3:24:E0:E5:9F:BE:91:B3:25:73:CB:00:65:78:D4:F6:D4:46:EF:F9:60:A1:28:C4:5E:C1:8F:8D:A6:A4:71:01:46:0F:0F:25:2F:1E:47:D3:54:2B:9E:A1:FE:F6:C2:11:5A:1B:97:D9:37:E8:F4:32:D5:22:41:29:11:0E:0E:93:EA:0E:E3:DD:43:00:20:33:B6:10:2F:3F:C5:61:5E:B6:F4:8D:11:BE:01:0E:7B:B9:EE:76:D8:14:16:E8:2A:39:B0:11:2F:BB:DB:05:01:B0:F2:E0:04:46:87:0A:90:FE:AF:11:99:B5:3A:26:3B:A3:EB:E5:CE:DD:0D:78:67:64:16:F8:61:38:ED:D3:9C:7D:81:64:A8:63:D2:DF:68:6E:03:02:32:28:A5:E4:ED:50:DC:77:24:EE:7B:42:6A:24:5C:0F:60:30:EF:51:63:0A:88:6A:35:DB:03:E0:ED:3E:E0:B2:7B:1F:3C:6A:DC:B8:B5:3F:2B:47:6F:AB:70:F8:38:16:26:63:A1:E8:12:53:F8:CC:35:EA:48:3C:F7:FB:15:00:F0:ED:0A:9D:5E:0A:6E:43:D1:5C:02:17:1E:BB:27:A2:3E:78:A0:41:D0:23:5B:08:8F:E5:31:F8:ED:F7:C1:36:80:67:8F:0D:BF:36:AF:3F:F5:43:60:69:17:1A:90:68:CD:C7:EB:02:03:01:00:01

Authority Info Access

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *70:E3:25:FD:CD:A9:72:3F:51:80:D6:22:7A:47:62:92:66:2E:BF:58*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.docuten.com/es/pcsc/cps/

CPS text: [Subordinate Certification Authority Certificate of / Certificado de la Autoridad de Certificacion Subordinada de / Docuten tech - www.docuten.com]

CRL Distribution Points

http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl

http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

Subject Alternative Name *info@docuten.com*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B0:CD:0C:09:3E:A1:D6:52:75:40:14:C6:AF:2E:2B:B2:1B:E1:83:8E:95:8E:90:6B:05:50:5E:CB:AD:60:BD:97*

X509SubjectName

Subject 2.5.4.97: *VATES-B85630978*

Subject CN: *DOCUTEN TECH CA1*

Subject OU: *TSP-PSC-DOCUTEN*

Subject O: *Docuten Tech SL*

Subject L: *A CORUÑA*

Subject C: *ES*

X509SKI

X509 SK I *cOMl/c2pcj9RgNYiekdikmYuv1g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-07-01T01:00:00Z*

44.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

44.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

44.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.56098.1.1.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.56098.1.2.2.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.56098.1.3.2*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.56098.1.4.2*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.56098.1.5.2*

Description

44.2 - Service (granted): Qualified electronic time stamps issued by "DOCUTEN timestamping electronic certificate – TSU01"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified electronic time stamps issued by "DOCUTEN timestamping electronic certificate – TSU01"*

Name [es] *Sellos electrónicos cualificados de tiempo emitidos por "DOCUTEN timestamping electronic certificate – TSU01"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2726984659801151553*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHIzCCBQugAwIBAgIIJdgyGZNjGEEwDQYJKoZIhvcNAQELBQAwgYoxCzAJBgNVBAYTAkVTMRIw
EAYDVQQHDAIBIENPUiXDkUExGDAWBgNVBAoMD0RvY3V0ZW4gVGVjaCBTTDEYMBYGA1UECwwPVFNQ
LVB1Qy1ET0NVVEVOMRkwFwYDVQQDDBBET0NVVEVOIFRFQ0gg00ExMRgwFgYDVQRhDA9WQVRFUy1C
ODU2MzA5NzgwHhcNMjAxMDA4MTAxODU0WhcNMjgxMDA4MTAxODU0WjCBrzELMAkGA1UEBhMCRVMx
EjAQBgNVBAcMCUEgQO9SVcORQTEYMBYGA1UECgwPRE9DVVRFTiBURUNIIFNMMRgwFgYDVQQLDA9U
U1AtUFNDLURPQ1VURU4xPjA8BgNVBAMMNURPQTVURU4gdGltZXN0YW1waW5nIGVšZWN0cm9uaWMg
Y2VydGlmaWNhdGUg4oCTIFRTVTAxMRgwFgYDVQRhDA9WQVRFUy1CODU2MzA5NzgwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCyOLdZ8FdoSedIOYFtXazZDb6Qlfzy4DU/IhTiizeRF3Me
QiTm7E0T4conOF1fxYSbft52zFrNHEkzJ8Shl2tY3JGuJzsQKstMQcRFIfmvmblVELhTClallmdR
uRzNbCAq1UELQ1LF+z3xyflumvL6BJhhhbEiem61tld3dSLKZXe4TeGoxDTJKQ8MRwjStc48OyoE
LLtFV2HagR/ZQUBJ39LCEmEGQR64JGWIZ1JffzDFDU+2DRcmHvhOtgwY6K3HBi3Ca0+qJICW3Aai
MpwCWRKKmtbHIZI00Kwf4pRcoGiGae/qy576JlkTcnnxN0DWerhXlYDlCqxZXvu0+s3AgMBAAGj
ggJkMIICYDB+BggrBgEFBQcBAQRyMHAwNgYIKwYBBQUHMAGGKmh0dHA6Ly9vY3NwMS51YW5hdGFj
YS5jb20vcHVibGlpL3BraS9vY3NwLzA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AyLnVhbmF0YWNh
LmNvbS9wdWJsaWMvcGtpL29jc3AvMB0GA1UdDgQWBBQBr4UVB0gWFRUAISgw6gNlaCsyFjAJBgNV
HRMEAjAAMB8GA1UdIwQYMBaAFHDjJ3NqXi/UYDWInpHYpmLr9YMBsGA1UdEgQUMBKBEGluZm9A
ZG9pdXRlbi5jb20wgaIGA1UdIASBgzCBgDCBlwYKKwYBBAGDhICCQCBiDAwBggrBgEFBQcCARYk
aHR0cHM6Ly93d3cuZG9jdXRlbi5jb20vZXMvcGNzYy9jcHMvMFQGCCsGAQUFBwICMEgeRgBUAGkA
bQBlAHMAdABhAG0AcABpAG4AZwAgAGUAbABlAGMAdAByAG8AbgBpAGMAIABjAGUAcgB0AGkAZgBp
AGMAYQB0AGUwCAYGBACPegECMH8GA1UdHwR4MHYwOaA3oDWGM2hbdHA6Ly9jcmwxLnVhbmF0YWNh
LmNvbS9wdWJsaWMvcGtpL2Nvb0C9kb2N1dGVuLmNvbDA5oDegNYYzaHR0cDovL2Nvb0ludWFuYXRh
Y2EuY29tL3B1YmxpYy9wa2kvY3JsL2RvY3V0ZW4uY3JsMA4GA1UdDwEB/wQEAwIHgDAWBgNVHSUB
Af8EDDAKBggrBgEFBQcDCDAbBgNVHREEFDASgRBpbmZvQGRvY3V0ZW4uY29tMA0GCSqGSIb3DQEB
CwUAA4ICAQCdvyKJ1wnCBrr7oF8Movcyi3vkqpbkcounhz0cxxFe/kMY+B4nozJq+ntPgT6cCPaD
re88uLOEVTSw5i11tpbk6QtCj5+0c75DK44qnKt8IcTwi+tJaBwMuYDIzdw3Q3MRH56+bSHdz
rYMhzZlm1SJAgBZqRqIXF7O6VGTkSPD7CmXR4sB4/O8BAJONmNDX6243Y3NUj8SxFsTbToQi8eFc
U4n6w9Zt9K7U95McSgyJthwdFnr+4cOJI4QqmmDiqx/phwrmeUW6gklbbXS7ySMMdD/WaCQKxxT3
N8+AyX9DPYSDWzZSr0rLOTU+ZnDm8CsKcX73VAvTnzy8tjG/RT9nA5kJcs0+YX4UeVMcMOuKDrb1
13acGItp1bUVPDq4tMOwBaRK3jn266DmHNiIQe5vYbSbLuIddPlZmPcCIQ9CDsAiTesqNpxgr9B1NO
qKiMG+l04Iyu1BpqXZPANFiLr7Bx0hRtwzVFWTBKaOUVcND+Jx1VLvxo/YvTa9mxuq85FY8wdRmB
L/4vtG5XFmrSJzdPhppq10adDQlSN2FUGdevBed2TSEL7AF3KUJNGqUwE89/QcBBiPXqcaCMbEeV
GUHcLgfeLrPxHAbPlbRx1+vEh1B0IZ8m0y0cRigY75mjpeJQWzkLRe7LUaO935TYE5YK1ejPAVnT
ZyPMgFtF5A==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-B85630978*

Issuer CN: *DOCUTEN TECH CA1*

Issuer OU: *TSP-PSC-DOCUTEN*

Issuer O: *Docuten Tech SL*

Issuer L: *A CORUÑA*

Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-B85630978*
Subject CN:	*DOCUTEN timestamping electronic certificate – TSU01*
Subject OU:	*TSP-PSC-DOCUTEN*
Subject O:	*DOCUTEN TECH SL*
Subject L:	*A CORUÑA*
Subject C:	*ES*
Valid from:	*Thu Oct 08 12:18:54 CEST 2020*
Valid to:	*Sun Oct 08 12:18:54 CEST 2028*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:38:B7:59:F0:57:68:49:E7:48:39:81:6D:5D:A6:75:0D:BE:90:95:FC:F2:00:35:07:B5:38:A2:CD:EF:D1:17:73:1E:42:24:E6:EC:4D:13:E1:CA:27:38:52:1F:C5:84:9B:7E:DE:76:CC:5A:CD:1C:49:33:27:C4:A1:B7:6B:58:DC:91:AE:27:3B:10:2A:C7:CC:41:C4:45:21:F9:AF:99:B9:55:10:B8:53:0A:56:A5:96:67:51:B9:1C:CD:6C:20:2A:D5:41:0B:43:52:C5:FB:3D:F1:C9:F9:6E:9A:F2:FA:04:96:E1:85:B1:22:7A:6E:B5:B6:57:77:75:22:CA:65:77:B8:4D:E1:A8:C4:34:C9:29:0F:0C:47:08:D2:B5:CE:3C:3B:2A:04:2C:BB:45:57:61:DA:81:1F:D9:41:40:49:DF:D2:C2:12:61:06:41:1E:B8:24:65:88:67:52:5F:7E:00:C5:0D:4F:B6:0D:17:A6:1E:F8:4E:B6:0C:18:E8:AD:C7:06:2D:C2:6B:4F:AA:24:80:96:DC:06:A2:32:9C:02:59:12:8A:99:F6:C7:64:8D:34:2B:01:78:A5:17:28:1A:D1:9A:7B:FA:B2:E7:BE:89:8A:59:13:72:78:B1:37:40:D6:7A:B8:57:95:80:E2:0A:AC:59:5E:5B:DA:D3:EC:77:02:03:01:00:01*
Authority Info Access	*http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*01:AF:82:55:07:48:16:15:15:00:95:28:30:EA:03:48:68:2B:32:16*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*70:E3:25:FD:CD:A9:72:3F:51:80:D6:22:7A:47:62:92:66:2E:BF:58*
Issuer Alternative Name	*info@docuten.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.56098.2.10* *CPS pointer: https://www.docuten.com/es/pcsc/cps/* *CPS text: [Timestamping electronic certificate]* *Policy OID: 0.4.0.2042.1.2*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/docuten.crl* *http://crl2.uanataca.com/public/pki/crl/docuten.crl*
Extended Key Usage	*id_kp_timeStamping*
Subject Alternative Name	*info@docuten.com*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *64:B2:6E:B2:72:6D:47:CA:A4:95:2F:E1:C2:88:E0:59:9E:94:5B:C7:DC:56:03:16:16:85:0B:4A:FB:39:A7:E6*

X509SubjectName

Subject 2.5.4.97: *VATES-B85630978*

Subject CN: *DOCUTEN timestamping electronic certificate – TSU01*

Subject OU: *TSP-PSC-DOCUTEN*

Subject O: *DOCUTEN TECH SL*

Subject L: *A CORUÑA*

Subject C: *ES*

X509SKI

X509 SK I *Aa+CVQdIFhUVAJUoMOoDSGgrMhY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-07-01T01:00:00Z

45 - TSP: MAILTECK, S.A.

.

TSP Name

Name	[es]	*MAILTECK, S.A.*
Name	[en]	*MAILTECK, S.A.*

TSP Trade Name

Name	[en]	*MAILTECK*
Name	[en]	*VATES- A31501901*
Name	[en]	*Mailteck SA*

PostalAddress

Street Address	[en]	*Polígono Industrial La Laguna, Avenida de la Recomba 14*
Locality	[en]	*Leganés*
State Or Province	[en]	*Madrid*
Postal Code	[en]	*28914*
Country Name	[en]	*ES*

PostalAddress

Street Address	[es]	*Polígono Industrial La Laguna, Avenida de la Recomba 14*
Locality	[es]	*Leganés*
State Or Province	[es]	*Madrid*
Postal Code	[es]	*28914*
Country Name	[es]	*ES*

ElectronicAddress

URI	[en]	*mailto:infomadrid@mailteck.com*
URI	[en]	*https://comunicaciones-legales.mailteck.com/*
URI	[es]	*https://comunicaciones-legales.mailteck.com/*

TSP Information URI

URI	*[en]*	*https://comunicaciones-legales.mailteck.com/*
URI	*[es]*	*https://comunicaciones-legales.mailteck.com/*

45.1 - Service (granted): Servicio cualificado de entrega electrónica certificada emitido para ‘’CertySign MAILTECK”

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description	*[en]*	*An electronic delivery service providing qualified electronic deliveries.*
	[es]	*Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name	*[es]*	*Servicio cualificado de entrega electrónica certificada emitido para ‘’CertySign MAILTECK”*
Name	*[en]*	*Qualified electronic certified delivery service issued for "CertySign MAILTECK"*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *8514469021950128893*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH3TCCBcWgAwIBAgIIdil4dsBnsv0wDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJjZWxvbmEgKHVlZSBjdXJyZWS0lGFkZUIlc3MgY XQgd3dLnVbbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQUSBVEFDQSBDQTEgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2N2xNDk5MB4X
DTIxMDIxMjEzMjMwMFoXDTI2MDIxMTEzMjMwMFowZTELMAkGA1UEBhMCRVMxFDASBgNVBAoMC01h
aWx0ZWNzIFNBMRIwEAYDVQQFEwlBMzE1MDE5MDExfjAQBgNVBAMMCUNlcnR5L2lnbjEYMBYGA1UE
YQwPVkFURVMtQTMxNTAxOTAxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn2K8IZvD
csPHxNRwAlNJnYw3rtsO3gOFavCdx1at575vP7L0dvCCN11Hbl6bb5fhPRd2S0nubW6FiYlO6ymP
xp82t5TpKXg9zleCsnrwy/WjDB49CMX1ctqJIuj/46JthLmxemIBSZ8mb/ivgAnaM8Il30s59EA/G
v/Dd6tTldt06eJy/N1LGr7Z4ZPNWX45nXsLaHXuoByhDuhlQVDZBGOuPSZ5U7kXsPWRD7tuQMRv
MXA5rsvaO6ilL8IVMTpYAEGzO+cOQ0RsbTNRFzK9MT6dZJso9THHACzsKV06kbbVa55LI3eO3hR
I3BMysIRCoAY4qhz7gG+G7L5+j/qwwIDAQABo4IDOzCCAzcwfAYIKwYBBQUHAQMEcDBuMAgGBgQA
jkYBATALBgYEAI5GAQMCAQ8wCAYGBACORgEEMDYGBgQAjkYBBTAsMCoWJGh0dHBzOi8vd3d3LnVh
bmF0YWNhLmNvbS9wdWJsaWMvY3BzLxMCRU4wEwYGBACORgEGMAkGBwQAjkYBBgIwgdcGCCsGAQUF
BwEBBIHKMIHHHMFUGCCsGAQUFBzAChkIodHRwOi8vd3d3LnVbbmF0YWNhLmNvbS9wdWJsaWMvZG93
bmxvYWQvdHNwX2NlcnRpZmljYXRlcy9zdWJvcmRpbmF0ZTEuY3J0MDYGCCsGAQUFBzABhipodHRw
Oi8vb2NzcDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUHMAGGKmh0dHA6
Ly9vY3NwMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAdBgNVHQ4EFgQUb9ulmB8ZnEua
+A14BYy6rV8TFocwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBQtce+wY3/1eCDlkRRBAwgU9N
5TCBmQYDVR0gBIGRMIGOMAkGBwQAi+xAAQMwgYAGCysGAQQBgyE2AQkGMHEwMAYIKwYBBQUHAgEW
JGh0dHBzOi8vd3d3LnVhbmF0YWNhLmNvbS9wdWJsaWMvY3BzLzA9BggrBgEFBQcCAjAxDC9RdWFs
aWZpZWQgY2VvdGlmaWNhdGUgZm9yIGUtc2VhbCBpbiBSZW1vdGUgUVNDRDCBjwYDVR0fBIGHMIGE
MECgPqA8hjpodHRwOi8vY3JsMS51YW5hdGFjYS5jb20vcHVibGljL3Bra S9jcmwv Q0Exc3Vib3Ik
aW5fZGEuY3JsMECgPqA8hjpodHRwOi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3Bra S9jcmwv
Q0Exc3Vib3JkaW5hZGEuY3JsMA4GA1UdDwEB/wQEAwIF4DAdBgNVHSUEFjAUBggrBgEFBQcDAgY1
KwYBBQUHAwQwMgYDVR0RBCswKYEnY29tdW5pY2FjaW9uZXNjZXJ0aWZpY2FkYXNAbWFpbHRlY2su
Y29tMA0GCSqGSIb3DQEBCwUAA4ICAQDRSE+o3xOqQK0DJZgyHMOAwEIB7EFlIbMWFeLPQSE4QI
GEHIbID0Ub0TxNFRwWUfQGr0/NuoIUOP3bs375K/v0VjByNqPlOgSCcQLdMbVVzwPXs40DXl/W
IQm7sXyu8Uoynkz5M1P84RGKflh35VmGt3dCTZa6ckSM5hIhbC4sumoycuZstiLNhDhNang1m4dO
BANQKJdN65AnpFhSRnyo8iPCr/2MCBIWuKCS18rLE3jflhcrA8c36b/TxR5G50nP30p3yDFSRcNy
oImDNiotPr1WQS3AqMssTfn62q3/9iOYOnSHg9NAIE0MhKaIGmEFzc94Ju1TIB+xsk8RHYlnaGA
CR2HKdHkKm24wW+f7XpRNJamLA3LDeJ+0Z0p9gSIBVIZcFpD2cUFWIrMgXv0zojPQuhMyrCKWoo
ErrJvQXRcV8L7tuAEVINs9/I0VS7NHPJTSOdw7aMu1C3pKzPpjuRE8VacnO0XdHLbX4wGGfWhgOA
HVoQtchaeuqIaXs6Lg3OGsOH9Xr+6N2bm4ywpy3SVTY2xm6tKWlKfjRBDy6ie2rKLcBC/zB4TnC2
gIS2dJg8DswNFrVk5sr8kYj5xeKSY7OLA7ndRqMADib26xEDMQKbAv0IoZ2P1bYQ+I0zV0yv936R
P8QIPr/iFp5LGMcGEIDe6u+lC0Xhrw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA1 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-A31501901*
Subject CN:	*CertySign*
Subject SERIAL NUMBER:	*A31501901*
Subject O:	*Mailteck SA*
Subject C:	*ES*
Valid from:	*Fri Feb 12 14:23:00 CET 2021*
Valid to:	*Wed Feb 11 14:23:00 CET 2026*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9F:62:BC:7D:9B:C3:72:C3:C7:C4:D4:70:02:53:49:9D:8C:37:AE:DB:0E:DE:03:85:6A:F0:9D:C7:56:AD:E7:BE:6F:3F:B2:F4:76:F0:82:37:5D:47:6C:8E:9B:6F:97:E1:3D:17:76:4B:49:EE:6D:6E:85:89:89:4E:EB:29:CF:C6:9F:36:B7:94:E9:29:78:3D:CE:57:82:B2:7A:F0:CB:F5:A3:0C:1E:3D:08:C5:F5:72:DA:89:22:E8:FF:E3:A2:6D:84:B9:B1:7A:62:01:49:9F:26:6F:F8:AF:80:09:DA:33:C2:37:D2:CE:7D:10:0F:C6:8B:F0:DD:E9:F7:F5:77:4B:7A:78:9C:BF:37:52:C6:B7:B6:78:64:F3:56:5F:8E:67:7D:7B:0B:68:75:EE:A0:1C:A1:0E:E8:65:41:50:D9:04:63:AE:3D:26:79:20:9E:E4:5E:C3:D6:44:3E:EE:40:C4:6F:31:70:39:AE:CB:DA:3B:A9:74:2F:C2:15:31:3A:58:00:41:B3:3B:E8:82:39:0F:11:B2:14:CD:44:5C:CA:F4:CE:DB:E1:92:6C:A3:D1:C7:B4:00:B3:B2:45:74:EA:46:DB:55:AE:79:2E:2D:DE:3B:78:51:23:70:4C:CA:C2:11:0A:80:18:E2:A8:73:EE:01:BE:1B:B2:F9:FA:3F:EA:C3:02:03:01:00:01*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15* *id_etsi_qcs_QcSSCD*
Authority Info Access	*http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt* *http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*87:DB:A5:98:1F:19:9C:48:9A:F8:02:38:F1:8C:BA:AD:5F:13:16:87*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*
Certificate Policies	*Policy OID: 0.4.0.194112.1.3* *Policy OID: 1.3.6.1.4.1.47286.1.9.6* *CPS pointer: https://www.uanataca.com/public/cps/* *CPS text: [Qualified certificate for e-seal in Remote QSCD]*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl* *http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl*
Extended Key Usage	*id_kp_clientAuth*
Subject Alternative Name	*comunicacionescertificadas@mailteck.com*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *46:3B:20:D1:F6:C5:71:8A:4E:5D:22:A5:FC:3D:09:DC:83:2E:2A:2C:C7:50:1F:AE:6D:5B:EE:B8:2B:2B:1D:B5*

X509SubjectName

Subject 2.5.4.97: *VATES-A31501901*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *A31501901*

Subject O: *Mailteck SA*

Subject C: *ES*

X509SKI

X509 SK I *h9ulmB8ZnEia+AI48Yy6rV8TFoc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-09-01T01:00:00Z

46 - TSP: CUSTOMER COMMUNICATIONS TECKNALIA, S.L.

.

TSP Name

Name	*[es]*	*CUSTOMER COMMUNICATIONS TECKNALIA, S.L.*
Name	*[en]*	*CUSTOMER COMMUNICATIONS TECKNALIA, S.L.*

TSP Trade Name

Name	*[en]*	*CUSTOMER COMMS*
Name	*[en]*	*VATES-B86414000*
Name	*[en]*	*CUSTOMER COMMUNICATIONS TECKNALIA SL*

PostalAddress

Street Address	*[en]*	*Polígono Industrial La Laguna, Avenida de la Recomba 14*
Locality	*[en]*	*Leganés*
State Or Province	*[en]*	*Madrid*
Postal Code	*[en]*	*28914*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*Polígono Industrial La Laguna, Avenida de la Recomba 14*
Locality	*[es]*	*Leganés*
State Or Province	*[es]*	*Madrid*
Postal Code	*[es]*	*28914*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:info@customercomms.com*
URI	*[en]*	*https://www.customercomms.com*
URI	*[es]*	*https://www.customercomms.com*
URI	*[es]*	*mailto:info@customercomms.com*

TSP Information URI

URI	*[en]*	*https://comunicaciones-legales.customercomms.com*
URI	*[es]*	*https://comunicaciones-legales.customercomms.com*

46.1 - Service (granted): Servicio cualificado de entrega electrónica certificada emitido para ‘’CertySign CUSTOMERSCOMMS”

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description	*[en]*	*An electronic delivery service providing qualified electronic deliveries.*
	[es]	*Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name	*[es]*	*Servicio cualificado de entrega electrónica certificada emitido para ‘’CertySign CUSTOMERSCOMMS”*
Name	*[en]*	*Qualified electronic certified delivery service issued for "CertySign CUSTOMERSCOMMS"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1468288520352863400*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH+zCCBeOgAwIBAgIIFGBooUNqlKgwDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJlZWxvbmEgKHNlZSBidXlyZWS0IGFkZXIlc3MgYXQgd3dLnVbbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQUSBVEFDQSBDQTEgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzlxNDk5MB4X
DTIxMDIxMjEzMjEwMFoXDTI2MDIxMTEzMjEwMFowijELMAkGA1UEBhMCRVMxLTArBgNVBAoMJENV
UlRPTUVSIENPTUUVTkIDQVRJT05TIFRFQ0tOQUs/QSBTTDESMBAGA1UEBRMJQjg2NDE0MDAwMRIw
EAYDVQQDDAlDZXJ0eVNpZ3AxGDAWBgNVBGEMD1ZBVEYTLU4NjQxNDAwMDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALoHeF+d04oEoMGEncyckDaK4SSi7t/QkAHdlmXkKYytTZrwA7du
EyAtC50suoXVDELuqubpYK4r/9ciR7qMkBCyH6N5mcuSDVKwF6+q3troR4u1SyX6Tc3anK7mOQFZ
rPh4UXOuLzuq/ARAmcDhJ/+J45f1NH6xMgw0tXo+2nZP0QDmS26ZWWr2ckt/38B5qXxe7xTlGOD4
3Sw4BnRtBBTOrq/Twfgm0bEFHIkwAthLh3z0lE29trJyIovdZfOUYG7bz+iPRQY3DCRC0fBXcmtWSK
0Pyv0d+CHd2nVGaukLp9IuM4NLh3RlFIv2dn383KF3StDku77FkK8WU3ldfO9skCAwEAAaOCA0Aw
ggM8MHwGCCsGAQUFBwEDBHAwbjAIBgYEAI5GAQEwCwYGBACORgEDAgEPMAgGBgQAjkYBBDA2BgYE
AIS6AQUwLDAqFiRodHRwczovL3d3dy51YW5hdGFjYS5jb20vcHVibGljL2Nwcy8TAkVOMBMGBgQA
jkYBBjAJBgcEAI5GAQYCMIHXBggrBgEFBQcBAQSByjCBxzBVBggrBgEFBQcwAoZIaHR0cDovL3d3
dy51YW5hdGFjYS5jb20vcHVibGljL2Rvd25sb2FkL3RzcF9jZXJ0aWZpY2F0ZXMvc3Vib3JkaW5h
dGUxLmNydDA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtp
L29jc3AvMDYGCCsGAQUFBzABhipodHRwOi8vb2NzcDludWFuYXRhY2EuY29tL3B1YmxpYy9wa2kv
b2NzcC8wHQYDVR0OBBYEFNoq49uJ0NDuqnJqAGoDqZCanEhvQMAwGA1UdEwEB/wQCMAAwHwYDVR0j
BBgwFoAULXHvsGN/9I3ggyJEf0QQMIFPTeUwgZkGA1UdIASBk1CBjjAJBgcEAIvsQAEDMIGABgsr
BgEEAYLxNgEJBjBxMDAGCCsGAQUFBwIBFiRodHRwczovL3d3dy51YW5hdGFjYS5jb20vcHVibGlj
L2Nwcy8wPQYIKwYBBQUHAgIwMQwvUXVhbGlmaWVkIGNlcnRpZmlj YXRlIGZvcyBlLXNlYWwgaW4g
UmVlb3RlIFFTQ0QuaYXGA1UdIwSBhzCBhDBAoD6gPIY6aHR0cDovL2NybDIudWFuYXRhY2EuY29t
L3B1YmxpYy9wa2kvY3JsL0NBMXN1Ym9yZGluYWRhLmNybDBAoD6gPIY6aHR0cDovL2NybDIudWFu
YXRhY2EuY29tL3B1YmxpYy9wa2kvY3JsL0NBMXN1Ym9yZGluYWRhLmNybDAOBgNVHQ8BAf8EBAMC
BcAwHQYDVR0IBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMDcGA1UdEQQwMC6BLGNvbXVuaWNhY2lv
bmVzY2VydGlmaWNhZGFzQGN1c3RvbWVyY29tbXMuY29tMA0GCSqGSIb3DQEBCwUAA4ICAQDQJcn3
tbgyYWNpR8ksbmMT7n4lG21HVrQdI3TDOK8As5Ha3PWLNqzBwCgY5Th5DqpN2ZoOOUzH9s1u17
jcam+oR/7pGiWzEqecASkg5oq3woDpYbGuSfUScLljTutNZNwEg+OSlSpHssL8ddwC4fgP9vZu7n
qNCaeFK4kUWcXNh3Ex/49ro0XbqadSINNBVYjrOJFI/7vnJr1HnLr+aPlgx3qKWQZ1na3ml/oFW9
9lgh6aZXPSUjd7owOcXYzGW24raJEMXmOzxDluXifRR6XqsAVW2BcqVU/WSacyV97DibBZlJUVkk
cRdcAT76pgFvrgLtcHXtxuMO4jkctIysPNqFnRy1ZIeJoxZIjRB5GFHsq4kJ9b/gZ0l3lms1oiq
5KDDNynwxMESk4b7beTmMXs4iFsCU8Zc9kAVcGv/j6eiKGvsqrVoWjB5AMRktA04sybqLU2Zd7G+
R6sAHJKCVa6KNpp1cXNPsv/YrTeR/LaVOtUEUR+/HB5b3k+WKXQimJ3zmmZiAwqPbMf6XBYqzojW
JjIlh/Vldy0kMyD3SzqBWdhhRQvObe08J3F2T2VHgmE3AKogIDzTGoeuuF5B4RT87iDYngcSgcub
pt0svp3kWGNdV/Mdd+kVcykz1RqMrq39IvQ5ENtEzFLRuTXzYqIc80OcWZRWt+wld0WA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA1 2016*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L:	*Barcelona (see current address at www.uanataca.com/address)*
Issuer C:	*ES*
Subject 2.5.4.97:	*VATES-B86414000*
Subject CN:	*CertySign*
Subject SERIAL NUMBER:	*B86414000*
Subject O:	*CUSTOMER COMMUNICATIONS TECKNALIA SL*
Subject C:	*ES*
Valid from:	*Fri Feb 12 14:21:00 CET 2021*
Valid to:	*Wed Feb 11 14:21:00 CET 2026*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:07:78:5F:9D:D3:8A:04:A0:C1:84:9D:EC:9C:90:36:8A:E1:24:A2:EE:2F:D0:90:01:DD:22:65:E4:29:8C:AD:4D:9A:F0:01:37:6E:13:20:2D:0B:9D:2C:BA:85:D5:0C:42:EE:AA:E6:E9:60:AE:2B:FF:D7:22:47:BA:8C:90:10:B2:1F:A3:79:99:CB:92:0D:52:B0:17:AF:AA:DE:DA:E8:47:8B:B5:4B:25:FA:4D:CD:DA:9C:AE:E6:39:01:59:AC:F8:78:51:73:AE:2F:3B:AA:FC:04:40:99:C0:E1:27:FF:88:E3:97:F5:34:7E:B1:32:AC:34:7D:7A:3E:DA:76:4F:D1:00:E6:4B:6E:99:59:6A:F6:72:4B:7F:DF:C0:79:A9:7C:5E:EF:14:E5:18:E0:F8:DD:2C:38:06:74:6D:04:14:F4:AE:AF:D3:C1:F8:26:D1:B7:FF:14:79:30:02:D8:4B:87:67:34:94:4D:BD:AC:9C:88:BA:F7:59:7C:E5:18:1B:B8:73:FA:23:D1:41:8D:C3:09:11:B4:05:77:26:B5:64:8A:D0:FC:AF:D1:DF:82:1D:DD:A7:54:66:AE:90:BA:7D:7C:9B:8C:E0:D2:E1:DD:19:45:22:FD:9D:9F:7F:37:28:5D:D2:B4:39:2E:EF:B1:64:F1:65:37:95:D7:CE:F6:C9:02:03:01:00:01*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_RetentionPeriod: 15* *id_etsi_qcs_QcSSCD*
Authority Info Access	*http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt* *http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*DE:AA:E3:DC:09:D0:D0:F0:A4:9B:80:1A:80:EA:64:26:AF:12:1B:D0*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*
Certificate Policies	*Policy OID: 0.4.0.194112.1.3* *Policy OID: 1.3.6.1.4.1.47286.1.9.6* *CPS pointer: https://www.uanataca.com/public/cps/* *CPS text: [Qualified certificate for e-seal in Remote QSCD]*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl* *http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl*
Extended Key Usage	*id_kp_clientAuth*
Subject Alternative Name	*comunicacionescertificadas@customercomms.com*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *04:2B:A1:E7:60:3B:28:12:F8:C1:25:2B:D1:29:D0:E5:21:F6:A2:A5:28:9A:08:36:89:F3:A5:EF:A5:28:5A:8C*

X509SubjectName

Subject 2.5.4.97: *VATES-B86414000*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *B86414000*

Subject O: *CUSTOMER COMMUNICATIONS TECKNALIA SL*

Subject C: *ES*

X509SKI

X509 SK I *3qrj3AnQ0PCkm4AagOpkJq8SG9A=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-09-01T01:00:00Z

47 - TSP: Iberexaminis Consulting S.L.

.

TSP Name

Name	*[en]*	*Iberexaminis Consulting S.L.*
Name	*[es]*	*Iberexaminis Consulting S.L.*

TSP Trade Name

Name	*[en]*	*EXAMINIS*
Name	*[es]*	*EXAMINIS*
Name	*[en]*	*VATES-B39877915*
Name	*[en]*	*Iberexaminis Consulting SL*

PostalAddress

Street Address	*[en]*	*CALLE JOAQUIN CAYON 14 4ºA*
Locality	*[en]*	*TORRELAVEGA*
State Or Province	*[en]*	*CANTABRIA*
Postal Code	*[en]*	*39300*
Country Name	*[en]*	*ES*

PostalAddress

Street Address	*[es]*	*CALLE JOAQUIN CAYON 14 4ºA*
Locality	*[es]*	*TORRELAVEGA*
State Or Province	*[es]*	*CANTABRIA*
Postal Code	*[es]*	*39300*
Country Name	*[es]*	*ES*

ElectronicAddress

URI	*[en]*	*mailto:info@iberexaminis.com*
URI	*[en]*	*https://www.iberexaminis.com*

TSP Information URI

URI	*[en]*	*https://iberexaminis.com/index.php/quienes-somos*
URI	*[es]*	*https://iberexaminis.com/index.php/quienes-somos*

47.1 - Service (granted): Qualified electronic time stamps issued by "Examinis TSU01"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[es]	*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name	*[en]*	*Qualified electronic time stamps issued by "Examinis TSU01"*
Name	*[es]*	*Sellos electrónicos cualificados de tiempo emitidos por "Examinis TSU01"*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *8182055068043534744*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHFTCCBP2gAwIBAgIIcYx/u+drYZgwDQYJKoZIhvcNAQELBQAwgbgxCzAJBgNVBAYTAkVTMUQw
QgYDVQQHDDtCYXJlZWxvbmEgKHNlZSBjdXJvZW50IGFkZHJlc3MgYXQgd3d3LnVhbmF0YWNhLmNv
bS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0EgUy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNB
MRowGAYDVQQDDBFVQU5BVEFDQSBDQTIgMjAxNjEYMBYGA1UEYQwPVkFURVMtQTY2NzIxNDk5MB4X
DTIxMDExNDEyMTgwMVoXDTI5MDExNDEyMTgwMVowgZYxCzAJBgNVBAYTAkVTMRQwEgYDVQQHDAtU
b3JyZWxhdmVnYTEjMCEGA1UECgwaSWJlcmV4YWJpbmlzIENvbnN1bHRpbmcgI0wxGTAXBgNVBAsM
EEICRVJFWEFNSU5JUyBUU1AxFzAVBgNVBAMMDkV4YWJpbmlzIFRTVTAxMRgwFgYDVQRhDA9WQVRF
Uy1CMzk4Nzc5MTUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDz5z7YHQky2/Y/Q4+h
849WXOgfo7NA1A7PXQ27JSLEHIeBWioo19SimUTQ9Gt+WvJTwx+tILsJEAtgvLr3UvJFioMeioQ4
PisHGb+J2+DJVUQbsO6bQSWzrR3FbwhGuz4z0kuWn0A9nK734FTAa3A4b8B4L8HKDj38FpnyYV4
/6CP6/iKDds52LR788mSHyYsm0QeA5PstywR0SFIGyzPH1aGDLXjRw52XwhOR3nL62JwX8ClhzGH
2DlrA4mGFHcYXACxwrelKchEC8Yw8Rnhqxr Aw/B4rN7KZXivdB0qA1bW6TWmSZUH96AqvlZ/lyzC
JeTwrQ3b8D9EbkJ2RUV3AgMBAAGjggIBMIICPTB+BggrBgEFBQcBAQRyMHAwNgYIKwYBBQUHMAGG
KmhtdHAtcy9vY3NwMSS1YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwcLzAZBggrBgEFBQcwAYYq
aHR0cDovL29jc3AyLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AvMB0GA1UdDgQWBBR50sTP
VOCZOUV90xvhZ95uFsLcRjAJBgNVHRMEAjAAMB8GA1UdIwQYMBaAFH1X52BzzgdGqeKjaPDhEbJ0
knP9MIGTBgNVHSAEgYswgYgwfAYKKwYBBAGC8TYCBTBuMDoGCCsGAQUFBwICMC4MLENlcnRpZmlj
YWRsIGRlIHNlbGxvdGRlIHRpZW1wbyBlbGVydHLDs25pY2XuMDAGCCsGAQUFBwIBFiRodHRwczov
L3d3dy51YW5hdGFjYS5jb20vcHVibGljL2Nwcy8wCAYGBACPegECMIGPBgNVHR8EgYcwgYQwQKA+
oDyGOmh0dHA6Ly9jcmwxLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9DQTJzdWJvcmRpbmFk
YS5jcmwwQKA+oDyGOmh0dHA6Ly9jcmwyLnVhbmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9DQTJz
dWJvcmRpbmFkYS5jcmwwDgYDVR0PAQH/BAQDAgeAMBYGA1UdQEB/wQMMAoGCCsGAQUFBwMIMCAG
A1UdEQQZMBeBFWluZm9AaWJlcmV4YWJpbmlzLmNvbTANBgkqhkiG9w0BAQsFAAOCAgEASNjoAmST
rdJoCTuMl7tjhyEuW5pbivGJ4ScGmyFn0hX/RPsfqdrXQjOJ0SlHjstBz68rjf0lX+T+PopaM5M
eYstB5Gly9c8gNXTM6AhlCV5XLyzWN2RnAia V4lzvcZW5yDjYU1ce4HxBkVep/RzqDucWzK7dC+f
9h/j48vAkIYcLrRfdxi0kRmH57ib1l6VpLBRMxbRuPsySxsOPZ+IQzNu8V4GB+3YDmbnEojy4Scu
z0GrfbamkfBFYYzcZMeNizKQ/mTdo19Ho2v1Z5/1Ub9mGXH75swMQ+UFZSGCbyossqJAtxARwtaDQm
nYdimhJDtDcN+LWLvvUFGqYu1QFXHGtGtKi6Vdwkgu/zGt4cxFJt/T7/gwG0/XiszvDWygwOxDEO
oCnEMyh9mnOHZ/ClctaLs64Mty/H5a0XACviATZN+991yLJ9QaSHMG/8/nv6rbPlpui9fiBjulwo
cbVrEMSf0IG7tZyQuFK3r1Zelly9r88xCaYj8mJvaIrPU/bhFrBjpFGp+RRgF1+AZ2o3mbgjXEBFR
iFPMZnBhIFk/Qvyxc1tLuGRV70tRy25sVbhBjba+gTpY1DVqQRBx+fsKgH1O7RYEBDam1Q9yY
p0H4kjMCTgW5H89hENIuMqI4b0Y0LIwHsS9RXE96yKPje8Rsz2KlSGhUd75JD5bVs=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer 2.5.4.97:	*VATES-A66721499*
Issuer CN:	*UANATACA CA2 2016*
Issuer OU:	*TSP-UANATACA*
Issuer O:	*UANATACA S.A.*
Issuer L:	*Barcelona (see current address at www.uanataca.com/address)*
Issuer C:	*ES*

Subject 2.5.4.97:	*VATES-B39877915*
Subject CN:	*Examinis TSU01*
Subject OU:	*IBEREXAMINIS TSP*
Subject O:	*Iberexaminis Consulting SL*
Subject L:	*Torrelavega*
Subject C:	*ES*
Valid from:	*Thu Jan 14 13:18:01 CET 2021*
Valid to:	*Sun Jan 14 13:18:01 CET 2029*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F3:E7:3E:D8:1D:09:32:DB:F6:3F:43:8F:A1:F3:8F:56:5C:E8:1F:A3:B3:40:D4:0E:CF:5D:0D:BB:25:22:C4:1E:57:81:5A:2A:2E:D7:D4:A2:99:44:D0:F4:6B:7E:5A:F9:53:C3:1F:AD:20:BB:09:10:0B:60:BC:BA:F7:52:F2:45:7E:83:1E:8A:84:38:3D:FB:07:19:BF:89:DB:E0:DF:55:44:0E:B0:EE:A1:41:25:B3:AD:1D:C5:6F:08:46:BB:3E:33:D2:4B:96:9F:40:3D:C4:AE:F7:E0:54:C0:6B:70:38:6F:C0:78:2F:CF:C7:28:38:F7:F0:5A:62:C9:85:78:FF:A0:8F:EB:F8:8A:0D:DB:39:D8:B4:7B:F3:C9:92:1F:26:2C:9B:44:1E:03:93:EC:B7:2C:11:D1:21:65:1B:2C:CF:1F:56:86:0C:B5:E3:47:0E:76:5F:08:4E:47:79:CB:EB:62:70:5F:C0:A4:87:31:87:D8:39:6B:03:89:86:14:77:18:5C:00:B1:C2:B7:A5:29:C8:44:0B:C6:30:F1:19:E1:AB:1A:C0:C3:F0:78:AC:DE:CA:65:78:AF:74:1D:2A:03:56:D6:E9:35:A6:49:95:07:F7:A0:2A:BE:56:7F:97:2C:C2:25:E4:F0:AD:0D:DB:F0:3F:44:6E:42:76:45:45:77:02:03:01:00:01*
Authority Info Access	*http://ocsp1.uanataca.com/public/pki/ocsp/* *http://ocsp2.uanataca.com/public/pki/ocsp/*
Subject Key Identifier	*79:D2:C4:CF:54:E0:99:39:45:7D:D3:1B:E1:67:DE:6E:16:C2:DC:46*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.47286.2.5* *CPS text: [Certificado de sello de tiempo electrónico.]* *CPS pointer: https://www.uanataca.com/public/cps/* *Policy OID: 0.4.0.2042.1.2*
CRL Distribution Points	*http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl* *http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*
Extended Key Usage	*id_kp_timeStamping*
Subject Alternative Name	*info@iberexaminis.com*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*54:A9:49:39:DE:E1:89:3D:A5:74:AD:98:DB:46:B4:58:C0:22:82:1B:BE:AA:7A:78:02:47:2F:A3:46:75:2A:12*

X509SubjectName

Subject 2.5.4.97: *VATES-B39877915*

Subject CN: *Examinis TSU01*

Subject OU: *IBEREXAMINIS TSP*

Subject O: *Iberexaminis Consulting SL*

Subject L: *Torrelavega*

Subject C: *ES*

X509SKI

X509 SK I *edLEz1TgmTlFfdMb4WfebhbC3EY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-10-04T01:00:00Z

48 - Signature node - Id: id-73a0a44fafcde4814a896054cf4eb835

.

Signing Time *2021-10-26T09:34:56Z*

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *17149912202851399879*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIID0zCCAzigAwIBAgIJAO4AukjMGDjHMA0GCSqGSIb3DQEBCwUAMIGBMSswKQYDVQQDEyJTUEFO
SVNIIFRSVVNUIExJUlQgU0NIRU1FIE9QRVJBVE9SMQswCQYDVQQGEwJFUzEpMCcGA1UEChMgTUlO
SVNURVJlTyBERSBFQ09OT01JQSBZIEVNUFJFU0ExGjAYBgNVBAsTEVNFIEFWQU5DRSBESUdJVEFM
MB4XDTE4MTIwMTE2NDIzNVoXDTIzMTIwMTE2NDIzNVowgYExKzApBgNVBAMTIlNQQU5JU0ggVFJV
U1QgTEITVCBTQ0hFTUUgT1BFUkFUT1IxCzAJBgNVBAYTAkVTMSkwJwYDVQQKEyBNSU5JU1RFUkIP
IERFIEVDT05PTUlBIFkgRUlUQUkVTQTEaMBgGA1UECxMRU0lUgQVZBTkNFIERJR0lfQUwwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDwdC6107ZXBCwYqJ4XCk9uGjOFQ8hRvt6+GY9isAKt
KKIz8d3e6O9SQqVo9bf5ylSWmdW2Fqh0WE7ul/4lUjVYplum8Y4hWKZ7jfA0dd5MdNl46cNr4WuE
r8EgB+l9JZzWxJkJW6pJbRmHAAuThcfqGpSSpsKqcKTpUay4eZMmbbG0cXj02n0FFVpUsz1dihy
//qmEvo48/yOJn+tkN5vw1XNCwDjNZyuJvthKW56l/exfrg0Xczig0/8Rw+qNacGcM+zXcobDBuLy
IrGoqZbNk1kuDwcDdw0aM6bOpdzHmMIsUTqYCZUB7H0v1rz1qlHSTR7GsZov2mC0qVm73T0AgMB
AAGjTDBKMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgZAMB0GA1UdDgQWBBRRqeMcCSKPkvSll8cwaypk
5/HMjjARBgNVHSUECjAIBgYEAJE3AwAwDQYJKoZIhvcNAQELBQADggEBAOUEpP7J9Vpr/VXaF8PF
wNHYcxfUoyoaGQpBZaPn9r2sU41Qgn80zhmt0W34Z7vlNrmFOtUVAJGkdTNjNC1ODpTjMB6xK0
73MB3h6CjnWDjl0Jy8lXnrmtm3B8+gnxXTPiN4U6lthKkFoe/rCT0W6aYmnmSWnWV3zOBgJMqi
SDHD05SSHYHDvxMZT3LzFnqOHw1sckZWT7Ey2NrwqwptqtoKBP3yuvH91gPyvL6OhPzuzz7ApQC4
dqV1QSWIO0zsg00GTHLDl5f87fPnvdg9M4Its2rPQMk1JgColAt83gJ3AVikndnbNBaMkOheANS
w55qSZOmmPeQ3qbYIDo=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer OU: *SE AVANCE DIGITAL*

Issuer O: *MINISTERIO DE ECONOMIA Y EMPRESA*

Issuer C: *ES*

Issuer CN: *SPANISH TRUST LIST SCHEME OPERATOR*

Subject OU: *SE AVANCE DIGITAL*

Subject O: *MINISTERIO DE ECONOMIA Y EMPRESA*

Subject C: *ES*

Subject CN: *SPANISH TRUST LIST SCHEME OPERATOR*

Valid from: *Sat Dec 01 17:42:35 CET 2018*

Valid to: *Fri Dec 01 17:42:35 CET 2023*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F0:74:2E:B5:D3:B6:57:04:2C:18:A8:9E:17:0A:4F:6E:1A:33:85:43:C8:51:BE:DE:BE:19:8F:62:B0:02:AD:28:A2:33:F
1:DD:DE:E8:EF:52:42:A5:68:F5:B7:F9:CA:54:96:99:D5:B6:16:A8:74:58:4E:EE:97:FE:25:52:35:58:A4:8B:A6:F1:8E:21:58:A6:7B:8D:F0:34:75:DE:4C:74:D9:78:E9:C3:6B:E1:6B:84:AF:C1:20:07:E7:FD:25:9C:D6:C4:99:09:
5B:AA:49:6D:19:87:00:0B:93:85:C7:EA:1A:94:92:A6:C2:AA:70:A4:E9:51:AC:B8:79:93:22:99:B6:C6:D1:C5:E3:D3:69:F4:14:55:69:52:CC:F5:76:28:72:FF:FA:A6:12:FA:38:F3:FC:8E:26:7F:AD:90:DE:6F:C3:55:CD:0B:00:
E3:35:9C:AE:26:F7:E1:29:6E:7A:51:EC:5F:AE:0D:17:71:C8:E0:D3:FF:11:C3:EA:8D:69:E1:9E:33:EC:D7:7A:88:43:06:E2:F2:22:B1:A8:A9:96:CD:93:59:2E:0F:07:03:77:0D:1A:33:A6:CE:A5:DC:C7:98:C2:2C:51:3A:98:09:
95:01:EC:7D:2F:D6:BC:F5:AA:51:D2:4D:1E:C6:B1:9A:2F:DA:60:B4:A9:59:BB:DD:37:FF:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Subject Key Identifier *51:A9:E3:1E:09:29:0F:92:F4:88:97:C7:30:6B:2A:64:E7:F1:CC:8E*

Extended Key Usage *id-tsl-kp-tslSigning*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *98:4B:45:92:8C:A1:36:91:D0:06:A1:02:65:A7:4A:88:79:51:BB:7A:C1:78:E8:31:D3:12:A7:3A:06:C1:AA:76*